PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference F1318-1-T EP	**FOR FURTHER ACTION**	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
International application No. PCT/IB 96/00859	International filing date *(day/month/year)* 27/08/1996	(Earliest) Priority Date *(day/month/year)* 28/08/1995
Applicant FELDBAU, Ofra		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 2 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. □ **Certain claims were found unsearchable** (see Box I).

2. □ **Unity of invention is lacking** (see Box II).

3. □ The international application contains disclosure of a **nucleotide and/or amino acid sequence listing** and the international search was carried out on the basis of the sequence listing

   □ filed with the international application.
   □ furnished by the applicant separately from the international application,
   □ but not accompanied by a statement to the effect that it did not include matter going beyond the disclosure in the international application as filed.
   □ Transcribed by this Authority

4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   □ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☒ the text is approved as submitted by the applicant.
   □ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this International Search Report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is:
   Figure No. 1
   ☒ as suggested by the applicant.
   □ because the applicant failed to suggest a figure.
   □ because this figure better characterizes the invention.
   □ None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 96/00859

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A,0 516 898 (PITNEY BOWES INC.) 9 December 1992 cited in the application see abstract see column 2, line 34 - column 3, line 11 see column 4, line 24 - column 5, line 57 see figure 1 ---	1,27
A	D.W.DAVIES & W.L.PRICE: "SECURITY FOR COMPUTER NETWORKS" 1989 , JOHN WILEY & SONS , CHICHESTER (UK) XP002020015 cited in the application see page 130, line 25 - page 131, line 28 -----	1,27

□ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 2 December 1996	Date of mailing of the international search report 17.12.96
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Lydon, M

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
/IB 96/00859

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A-516898	09-12-92	US-A- 5022080	04-06-91

PCT/IB96/00859

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

United States Patent and Trademark
Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year)
22 April 1997 (22.04.97)

International application No.
PCT/IB96/00859

Applicant's or agent's file reference
F1318-1-TPCT

International filing date (day/month/year)
27 August 1996 (27.08.96)

Priority date (day/month/year)
28 August 1995 (28.08.95)

Applicant
FELDBAU, Ofra et al

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:

26 March 1997 (26.03.97)

□ in a notice effecting later election filed with the International Bureau on:

____

2. The election ☒ was
□ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
Ting Zhao

Telephone No.: (41-22) 730.91.11

9

TENT COOPERATION TREA

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference F1318-Tv1 PCT 96	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/ IB 96/ 00859	International filing date *(day/month/year)* 27/08/1996	Priority date *(day/month/year)* 28/08/1995
International Patent Classification (IPC) or national classification and IPC H04L9/32		
Applicant FELDBAU, Ofra		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consists of a total of 14 sheets.

3. This report contains indications and corresponding pages relating to the following items:

   I ☒ Basis of the report
   II ☐ Priority
   III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   IV ☐ Lack of unity of invention
   V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   VI ☐ Certain documents cited
   VII ☐ Certain defects in the international application
   VIII ☒ Certain observations on the international application

Date of submission of the demand 26/03/1997	Date of completion of this report 11.06.97
Name and mailing address of the IPEA European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Netherlands Tel.: (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Lydon, M.C.P. 02874 Telephone No. 0031-70-3403828

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/IB96/00859

I. Basis of the report

1. This report has been drawn up on the basis c: *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.)*

□ the international application as originally filed

☒ the description, pages 1-10,12-36 , as originally filed
pages , filed with the demand
pages 11,37,38 , filed with the letter of 09/05/97

☒ the claims, Nos. 59-63 , as originally filed
Nos. , as amended under Article 19
Nos. , filed with the demand
Nos. 1-58 , filed with the letter of 09/05/97

☒ the drawings, sheets / fig. 1/7-7/7 , as originally filed
sheets / fig. , filed with the demand
sheets / fig. , filed with the letter of

2. The amendments have resulted in the cancellation of:

□ the description, pages:

□ the claims, Nos.

□ the drawings, sheets / fig.

3. □ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2 (c)).

4. Additional observations, if necessary:

V. **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty	Claims	1 - 63	YES
	Claims		NO
Inventive Step	Claims	1 - 63	YES
	Claims		NO
Industrial Applicability	Claims	1 - 63	YES
	Claims		NO

2. Citations and Explanations

1. The following document has been considered for the purposes of this report:
D1: EP-A-516898

2. The invention relates to an apparatus (Claim 1) and a method (Claim 27) for authenticating that certain information has been sent by a sender via a dispatcher to a recipient i.e. it seeks to provide a sender with a proof of both the dispatch (i.e. dispatch time and destination information) and the contents of dispatched materials (paper documents, electronic information, etc.).

3. The closest prior art document (D1), cited on page 2 of the description, discloses a method and apparatus for the notarization of data wherein an authentication string (comprising both original data contents and dispatch information) is transmitted along with the electronic document to an intended recipient to prove that the document itself is valid and unmodified from a certified instant in time.

4. The problem with the apparatus and method of D1 is that it provides authentication information which is "document-related" rather than "dispatch-related" (e.g. the time information is used to time stamp or notarize the document content and is not specifically related either to the time/date of its transmission or to the dispatch destination).

5. The problem itself can be considered as inventive since there are no indications whatever in the prior art that would lead a skilled person to address the need for authenticated document dispatch. (The solution to this problem is obvious, however, namely to provide these additional information elements in some secure manner in the authentication string and in particular as

disclosed in independent claims 1 and 27.)

6. Claims 2 - 26 and claims 28 - 63 are dependent respectively on Claim 1 and Claim 27 and therefore also relate to novel and inventive subject-matter.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. The statement in the description on page 37, lines 28-30 is inconsistent with the definition of the matter for which protection is sought, contrary to Article 6 PCT.

Art. 34

In one embodiment of the present invention, the associated copies 24 and 34 are provided to the sender at this stage (where the dispatch sheet 26 is retained with the service to ascertain delivery and to fill in the proof of delivery indication 18) or after the delivery is completed. In another embodiment, the dispatch service retains, in a secure location 36, one or both of the copies 24 and 34.

The clerk 20 can also identify the authenticating party, for example via his signature, or by having the dispatch sheet copy 34 printed on the stationary of the dispatching service, by stamping the documents and/or dispatch sheet copies with the service's stamp, logo or seal, etc.

When it is desired to authenticate the dispatch of the original documents (and possibly also their receipt at the destination 30), either the sender or the document dispatching service provides the associated authentication-information, for example the envelope 32, unopened, to the party which required the authentication. When the envelope 32 is opened, it has associated therewith copies of both the dispatched documents and the dispatch information. The envelope 32 therefore, provides a reliable proof that the original documents 12 were dispatched on the date and to the destination listed on or in envelope 32.

It will be appreciated that, since a non-interested third party who is neither the sender nor the receiver copied the original documents 12 being sent, it is unlikely that the copies stored in the envelope 32 are other than copies of the original documents 12.

Various modifications can be made to the embodiment provided hereinabove. For example, the document copy could be sent to the destination while the original

Art. 34

[1.08] see [1] Chapter 24 Section 24.12, pp. 584-587.

[1.09] see [1] Chapter 3 Section 3.2, pp. 52-56.

[1.10] see [1] Chapter 4 Section 4.1, pp. 75-79.

[1.11] see [1] Chapter 21, pp. 503-512.

[1.12] see [1] Chapter 2, Sections 2.6-2.7, pp. 34-44, see also [1] Chapter 20, pp. 483-502.

[1.13] see [1] Chapter 18, Section 18.4, pp. 455-459.

[2] U.S. Patent Documents #5,136,646, #5,136,647, and #5,373,561.

[3] "Cyclic Redundancy Checksums (Tutorial)" (Louis, B. Gregory, C Users Journal, R & D Publications Inc., Oct 1992 v10 n10 p55 (6)), see also "File verification using C.R.C." (Nelson, Mark R., Dr. Dobb's Journal, M&T Publishing Inc., May 1992 Vol 17 No. 5 p64(6)).

[4] "The MD4 Message Digest Algorithm" (R. L. Rivest, Crypto '90 Abstracts, Aug. 1990, pp. 301-311, Springer-Verlag).

[5] "A Universal Algorithm for Sequential Data Compression" (Ziv. J., Lempel A., IEEE Transactions On Information Theory, Vol 23, No. 3, pp. 337-343).

The references and publications described by the above-mentioned articles are incorporated herein by reference.

Art. 34

While the present invention has been described with reference to a few specific embodiments, the description is illustrative of the invention as defined by the claims.

Art. 34

WHAT IS CLAIMED IS :

~~1. Apparatus for authenticating that certain information has been sent by a sender via a dispatcher to a recipient, the apparatus comprising:~~

~~means for providing a set A comprising a plurality of information elements a1,...,an, said information element a1 comprising the contents of said dispatched information, and said information elements a2,...,an comprising dispatch-related information and including at least the following elements:~~

~~a2 - a time indication associated with said dispatch; and~~

~~a3 - information describing the destination of said dispatch,~~

~~and wherein at least one of said information elements is provided in a manner that is resistant or indicative of tamper attempts by said sender;~~

~~means for associating said dispatch-related information with said element a1 by generating authentication--information, in particular comprising a representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; and~~

~~means for securing at least part of said authentication-information against undetected tamper attempts of at least said sender.~~

~~2. Apparatus according to claim 1, wherein said element a2 comprises at least one element of the group comprising the date associated with said dispatch, and the time associated with said dispatch.~~

40

3. Apparatus according to any of claims 1 or 2, wherein said dispatch-related information comprises at least one element of the group comprising the following elements: a completion indication associated with said dispatch, the number of pages dispatched, page number, an indication of identification associated with said sender, said dispatch duration, integrity information, an indication of dispatch identification associated with said dispatch, an indication of identification associated with said apparatus, a heading message, and a trailing message.

4. Apparatus according to any of claims 1 to 3, wherein said dispatched information has a form selected from the group comprising the following forms: a paper document and electronic information.

5. Apparatus according to any of claims 1 to 4, wherein the elements of said authentication-information and of said set A have a form selected from the group comprising the following forms: a paper document and electronic information, and where each of said elements can have different form.

6. Apparatus according to any of claims 1 to 5, wherein the information originally provided by said sender for dispatch has a form selected from a group comprising the following forms: a paper document and electronic information.

7. Apparatus according to any of claims 1 to 6, wherein said element a1 is provided by means comprising at least one of the following means: a communication network, a scanning device, a copier, a dispatcher, and a computer.

8. Apparatus according to any of claims 1 to 7, wherein said dispatcher comprises at least one element of the following group: a facsimile machine, a modem, a net-

Art.34

work interface card (NIC), a computer, a communication line, a communication network, an E-Mail system, an EDI system, and a dispatching service.

9. Apparatus according to claim 8, wherein said dispatching service comprises at least one element of the following group: a courier service, the registered mail service of the post office, and a message transmission forwarding service.

10. Apparatus according to any of claims 1 to 9, comprising means for providing said dispatched information to said dispatcher.

11. Apparatus according to any of claims 1 to 10, and comprising at least part of said dispatcher.

12. Apparatus according to any of claims claim 1 to 11, comprising means for preparing at least one element of the group comprising the elements of said set A, and said dispatched information.

13. Apparatus according to any of claims 1 to 12, wherein said element a3 comprises at least one element of the group comprising an address associated with said dispatch, an address associated with said recipient, and an indication of identification associated with said recipient.

14. Apparatus according any of claims 1 to 13, wherein at least part of said apparatus is resistant or indicative of tamper attempts by at least said sender.

15. Apparatus according to any of claims 1 to 14, comprising means for providing at least part of said authentication-information to an interested party.

Art. 34

16. Apparatus according to claim 15, wherein said interested party comprises at least one element of the following group: said sender, said recipient, an arbitrator, and a legal authority.

17. Apparatus according to any of claims 1 to 16, comprising means for storing at least part of said authentication-information.

18. Apparatus according to any of claims 1 to 17, comprising means for generating a new set B, said set B comprising one or more information elements b1,...,bm, each element bi comprising a representation of a subset Si, said representation being expressive as a function Fi of the elements of said subset Si, where said subset Si comprise a digital representation of at least one element of said set A, and where said functions Fi can be different.

19. Apparatus according to claim 18, wherein at least one element of said authentication-information comprise a representation of at least part of said new set B.

20. Apparatus according to any of claims 1 to 19, wherein said set A comprises a link information element, and wherein said authentication-information comprise at least one element which comprise a representation of at least said link element.

21. Apparatus according to any of claims 18 to 20, wherein said function Fi has the property that it is substantially difficult to find a set S′ comprising at least one information element, said set S′ being different from said subset Si and yet can be used instead, such that applying said function Fi to said set S′ will yield said element bi, i.e., such that Fi(S′)=bi.

Art 34

22. Apparatus according to any of claims 18 to 21, wherein said function Fi comprises one or more functions.

23. Apparatus according to any of claims 18 to 22, wherein at least one member of the group comprises the following members: said function Fi, and at least one information element of said new set B, is unknown at least to said sender.

24. Apparatus according to any of claims 1 to 23, comprising means for verifying the authenticity of an information element purported to match a corresponding element of said set A, said verification means comprises:

means for comparing a representation of said purported information element with a representation of at least part of said authentication-information which comprises a representation of at least said corresponding element of said set A to determine if they match.

25. Apparatus according to any of claims 18 to 24, comprising means for verifying the authenticity of a set Si' comprising one or more information elements which are purported to match the corresponding elements of said subset Si, said verification means comprises:

means for generating a new information element bi' comprising a representation of said set Si' which is expressive as said function Fi of the elements of said set Si'; and

means for comparing a representation of said element bi' with a representation of said element bi to determine if they match.

26. Apparatus according to any of claims 18 to 25, wherein said function Fi comprises at least one reversible function, comprising means for generating a set C which comprise one or more information elements c1,...,ck, where said set C is expressive as a function I of at least part

of said information element bi, and said function I comprises the inverse function of at least one of said reversible functions.

27. A method for authenticating that certain information has been sent by a sender via a dispatcher to a recipient, comprising the steps of:

providing a set A comprising a plurality of information elements a1,...,an, said information element a1 comprising the contents of said dispatched information, and said information elements a2,...,an comprising dispatch--related information and including at least the following elements:

a2 - a time indication associated with said dispatch; and

a3 - information describing the destination of said dispatch,

and wherein at least one of said information elements is provided in a manner that is resistant or indicative of tamper attempts by said sender;

associating said dispatch-related information with said element a1 by generating authentication-information, in particular comprising a representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; and

securing at least part of said authentication-information against undetected tamper attempts of at least said sender.

28. A method according to claim 27, wherein at least part of the activities described by said steps is performed by an authenticator, said authenticator comprising at least one element of the following group: a party other than said sender, said dispatcher, a device, and any combination thereof.

Art 34

~~29. A method according to any of claims 27 or 28, wherein said dispatch-related information comprises at least one element of the group comprising the following elements: a completion indication associated with said dispatch, the number of pages dispatched, page number, an indication of identification associated with said sender, said dispatch duration, integrity information, an indication of dispatch identification associated with said dispatch, an indication of identification associated with said authenticator, a heading message, and a trailing message.~~

~~30. A method according to any of claims 27 to 29, wherein said dispatched information has a form selected from the group comprising the following forms: a paper document and electronic information.~~

~~31. A method according to any of claims 27 to 30, wherein the elements of said authentication-information and of said set A have a form selected from the group comprising the following forms: a paper document and electronic information, and where each of said elements can have different form.~~

~~32. A method according to any of claims 27 to 31, wherein the information originally provided by said sender for dispatch has a form selected from a group comprising the following forms: a paper document and electronic information.~~

~~33. A method according to any of claims 27 to 32, wherein said element a1 is provided by means comprising at least one of the following means: a communication network, a scanning device, a copier, a dispatcher, and a computer.~~

34. A method according to any of claims 27 to 33, wherein said dispatcher comprises at least one element of the following group: a facsimile machine, a modem, a net-

Art 34

work interface card (NIC), a computer, a communication line, a communication network, an E-Mail system, an EDI system, and a dispatching service.

35. A method according to claim 34, wherein said dispatching service comprises at least one element of the following group: a courier service, the registered mail service of the post office, and a message transmission forwarding service.

36. A method according to any of claims 27 to 35, comprising the step of providing said dispatched information to said dispatcher.

37. A method according to any of claims 27 to 36, wherein said element a2 comprises at least one element of the group comprising the date associated with said dispatch, and the time associated with said dispatch.

38. A method according to any of claims 27 to 37, comprising the step of preparing at least one element of the group comprising the elements of said set A, and said dispatched information.

39. A method according to any of claims 27 to 38, wherein said element a3 comprises at least one element of the group comprising an address associated with said dispatch, an address associated with said recipient, and an indication of identification associated with said recipient.

40. A method according any of claims 27 to 39, comprising the step of dispatching said information to said recipient.

41. A method according to any of claims 27 to 40, comprising the step of providing a representation of at

Art. 34

~~least part of said authentication-information to an interested party.~~

~~42. A method according to claim 41, wherein said interested party comprises at least one element of the following group: said sender, said recipient, an arbitrator, and a legal authority.~~

~~43. A method according to any of claims 27 to 42, comprising the step of storing at least part of said authentication-information in a storage device.~~

~~44. A method according to any of claims 28 or 43, wherein at least part of said device is resistant or indicative of tamper attempts by at least said sender.~~

~~45. A method according to any of claims 27 to 44, comprising the step of generating a new set B, said set B comprising one or more information elements b1,...,bm, each element bi comprising a representation of a subset Si, said representation being expressive as a function Fi of the elements of said subset Si, where said subset Si comprise a digital representation of at least one element of said set A, and where said functions Fi can be different.~~

~~46. A method according to claim 45, wherein at least one element of said authentication-information comprises a representation of at least part of said new set B.~~

~~47. A method according to any of claims 27 to 46, wherein said set A comprises a link information element, and wherein said authentication-information comprise at least one element which comprise a representation of at least said link element.~~

48. A method according to any of claims 45 to 47, wherein said function Fi has the property that it is sub-

Art 34

stantially difficult to find a set S′ comprising at least one information element, said set S′ being different from said subset Si and yet can be used instead, such that applying said function Fi to said set S′ will yield said element bi, i.e., such that Fi(S′)=bi.

49. A method according to any of claims 45 to 48, wherein said function Fi comprises one or more functions.

50. A method according to any of claims 45 to 49, wherein at least one member of the group comprises the following members: said function Fi, and at least one information element of said new set B, is unknown at least to said sender.

51. A method according to any of claims 27 to 50, comprising the step of verifying the authenticity of an information element purported to match a corresponding element of said set A, said verification step comprises the step of:

comparing a representation of said purported information element with a representation of at least part of said authentication-information which comprises a representation of at least said corresponding element of said set A to determine if they match.

52. A method according to any of claims 45 to 51, comprising the step of verifying the authenticity of a set Si′ comprising one or more information elements which are purported to match the corresponding elements of said subset Si, said verification step comprises the steps of:

generating a new information element bi′ comprising a representation of said set Si′ which is expressive as said function Fi of the elements of said set Si′; and

comparing a representation of said element bi′ with a representation of said element bi to determine if they match.

Art 34

53. A method according to any of claims 45 to 52, wherein said function Fi comprises at least one reversible function, comprising the step of generating a set C which comprise one or more information elements c1,...,ck, where said set C is expressive as a function I of at least part of said information element bi, and said function I comprising the inverse function of at least one of said reversible functions.

54. Apparatus according to any of claims 18 to 26, wherein said new set B comprises a verifiable digital signature of said subset Si.

55. Apparatus according to claim 54, comprising a corresponding verification means for said verifiable digital signature, for authenticating at least one of the following: at least one element of said subset Si, and the originator of said digital signature.

56. Apparatus according to any of claims 54 or 55, wherein said digital signature is generated according to a scheme selected from the group comprising: secret-key (symmetric) cryptosystem, and public-key cryptosystem.

57. Apparatus according to any of claims 1 to 26, or 54 to 56, comprising means for time-stamping at least one element of the group comprising the elements of said authentication-information and the elements of said set A, according to a Time Stamping Service scheme.

58. Apparatus according to any of claims 1 to 26, or 54 to 57, comprising means for authenticating the identity of at least one member of the group comprising: said sender, said recipient, an agent of said sender, and an agent of said recipient.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32	A1	(11) International Publication Number: WO 97/08869 (43) International Publication Date: 6 March 1997 (06.03.97)

(21) International Application Number: PCT/IB96/00859

(22) International Filing Date: 27 August 1996 (27.08.96)

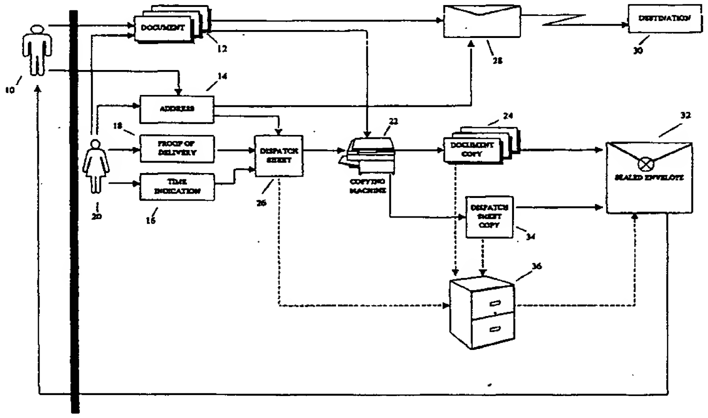
(30) Priority Data: 28 Feb 98
95113489.9 28 August 1995 (28.08.95) EP
(34) Countries for which the regional or international application was filed: AT et al.
117234 22 February 1996 (22.02.96) IL

(71)(72) Applicants and Inventors: FELDBAU, Ofra [IL/IL]; 12 Avtalyon Street, 52424 Ramat Gan (IL). FELDBAU, Michael [IL/IL]; 12 Avtalyon Street, 52424 Ramat Gan (IL).

(81) Designated States: AU, CA, CN, IL, JP, KR, MX, NZ, SG, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: APPARATUS AND METHOD FOR AUTHENTICATING THE DISPATCH AND CONTENTS OF DOCUMENTS



(57) Abstract

Apparatus and method for authenticating that a sender has sent certain information via a dispatcher to a recipient is disclosed. The method includes the steps of: (a) providing a set A comprising a plurality of information elements al, ..., an, said information element al comprising the contents of said dispatched information, and said one or more information elements a2, ..., an comprising dispatch-related information and comprise at least the following elements: a2 - a time indication associated with said dispatch; and a3 - information describing the destination of said dispatch, and wherein at least one of said information elements is provided in a manner that is resistant or indicative of tamper attempts by said sender; (b) associating said dispatch-related information with said element a1 by generating authentication-information, in particular comprising a representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; (c) securing at least part of said authentication-information against undetected tamper attempts of at least said sender. The dispatch relates either to transmission or to manual delivery. The apparatus implements the operations of the method.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 96/00859

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A,0 516 898 (PITNEY BOWES INC.) 9 December 1992 cited in the application see abstract see column 2, line 34 - column 3, line 11 see column 4, line 24 - column 5, line 57 see figure 1 ---	1,27
A	D.W.DAVIES & W.L.PRICE: "SECURITY FOR COMPUTER NETWORKS" 1989 , JOHN WILEY & SONS , CHICHESTER (UK) XP002020015 cited in the application see page 130, line 25 - page 131, line 28 -----	1,27

□ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search 2 December 1996	Date of mailing of the international search report 17.12.96
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Lydon, M

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 96/00859

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A-516898	09-12-92	US-A- 5022080	04-06-91

APPARATUS AND METHOD FOR AUTHENTICATING
THE DISPATCH AND CONTENTS OF DOCUMENTS

FIELD OF THE INVENTION

The present invention relates to a method and apparatus for authenticating the dispatch and the contents of dispatched information in general.

BACKGROUND OF THE INVENTION

Post, courier, forwarding and other mail services, which enable people to exchange documents and data, have been widely used both in the past and at the present time.

With the evolution of modern technology, the use of electronic dispatch devices and systems, such as modems, facsimile machines, electronic mail (E-Mail) and EDI systems, computers, communication networks, and so forth, to exchange data and documents is rapidly evolving.

A substantial quantity of the information exchanged, such as contracts, purchase orders, invoices, monetary orders, notices, and even warning and notification messages, are of utmost importance. Sometimes, when a dispute arises between the sending and receiving party of the exchanged information, the receiving party may raise the claim that he never received the information, that the received information was different from what the sender claims to have sent, or the receiving party may even attempt to forge the received information.

The need, therefore, arises for the sender to prove that specific information has been sent at a specific time to that specific receiving party.

מתקן ושיטה לאימות משלוח מסמכים ותוכנם

APPARATUS AND METHOD FOR AUTHENTICATING THE DISPATCH AND CONTENTS OF DOCUMENTS

Various solutions to various related problems have been proposed in the literature. For example, the transmission operation itself may be authenticated, as shown in US Patent 5,339,361 (Schwalm et al.), which describes a communication system providing a verification system to identify both the sender and recipient of electronic information as well as an automatic time stamp for delivery of electronic information. This patent, however, does not verify the dispatched information.

Document authentication methods, for example by notarization, have long been in use. A method for notarization of electronic data is provided by US Patent 5,022,080 (Durst et al.) which authenticates that source data has not been altered subsequent to a specific date and time. The method disclosed includes mathematically generating a second unit of data from the first unit of data, as by CRC generation, parity check or checksum. The second unit of data is then encrypted together with a time/date indication, and optionally with other information to form an authentication string. Validation that the first unit of data has not been changed is provided by comparing the original data's authentication string with the authentication string generated from the data and time in question. A method is even suggested for having the recipient verify the authenticity of the sender, the time of transmission and the data.

Other patents which discuss document authentication are U.S. 5,136,646 and 5,136,647 both to Haber et al. According to these patents, a unique digital representation of the document (which is obtained by means of a one-way hash function) is transmitted to an outside agency, where the current time is added to form a receipt. According to patent 5,136,647, the receipt is certified using a cryptographic digital signature procedure, and is optionally linked to other contemporary such receipts thereby fixing the document's position in the continuum of time. According to patent 5,136,646, the receipt is certified by concatenating and hashing the receipt with the current record catenate certificate which itself is a number obtained by sequential hashing of each prior receipt with the extent catenate certificate.

Various cryptographic schemes are known in the prior art for encrypting and for authenticating digital data and/or its author. For example Symmetric algorithms such as DES [1.01] and IDEA [1.02], one-way hash functions [1.03] such as MD5 [1.04], Public-Key (asymmetric) algorithms [1.05] such as RSA [1.06], and verifiable digital signatures generation algorithms [1.12] such as DSA [1.07] or RSA, as well as combinations thereof such as PGP [1.08] and MACs [1.13], are currently widely used for security and for authentication purposes [1.09]. An excellent publication relating to encryption, authentication, public-key cryptography and to cryptography and data security in general, as well as applications thereof and additional references to multiple sources can be found in [1].

Proof of delivery of non-electronic documents is provided, for example, by Registered Mail and courier services. It is commonly used to authenticate the delivery of materials at a certain time to a certain party, and serves as admissible proof of delivery in a court of law. However, no proof is provided as to the information contents of the specific dispatch.

E-mail and other electronic messages forwarding services are commonly used today. The sender sends a message to the dispatching service which, in turn, forwards the message to the destination and provides the sender with a delivery report which typically includes the date and time of the dispatch, the recipient's address, the transmission completion status, and sometimes even the transmitted data, the number of pages delivered, the recipient's identification information, and so on. The provided delivery report mainly serves for accounting purposes and for notifying the sender of the dispatch and/or its contents. Moreover, frequently no record of the specific dispatched data is maintained with the service after the delivery is completed or provided to the sender.

SUMMARY OF THE PRESENT INVENTION

The literature does not provide a comprehensive solution that directly addresses the problem in question: what information has been sent to whom and when. Accordingly, there is a need for a method and system to provide the sender with a convenient means for authenticating both the dispatch and the contents of documents, electronic information and other information during the normal flow of daily activities.

It is therefore an object of the present invention to improve the capacity of conventional systems and methods for dispatching documents and transmitting information to provide the sender with evidence he can use to prove both the dispatch and its contents.

The present invention discloses a method and apparatus for providing a sender with the capability to prove both the dispatch and the contents of the dispatched materials. The dispatched materials can be paper documents, electronic information or other information which can be dispatched electronically by transmission or non-electronically, such as by courier or registered mail service, to an address of a recipient.

According to the present invention, dispatch related information is associated with the contents of the dispatch, in a relatively secure, or reliable manner. This associated information can be provided for example to the sender, and may serve as evidence of both the dispatch and its contents, for example, in a court of law, and therefore it is collectively referred to herein as the "authentication information".

The present invention encompasses all types of information being dispatched, such as that found on paper documents or within electronic documents and other electronic data, and all types of dispatch methods, such as transmission via facsimile machines, modems, computer networks, electronic mail systems and so forth, or manually such as via registered mail or courier services.

The term "the contents of the dispatch" herein refers to any information element having information content the substance of which is equivalent to that of the information being dispatched. This includes for example the information source, either in paper document or electronic form, the actual dispatched information, any copies thereof, any descriptive information or portion of the information contents identifying the dispatched information, and so forth regardless of the representation or form.

The present invention also encompasses all types of methods and apparatuses which provide and/or associate the dispatch information with the contents in a relatively secure or reliable manner. The terms "relatively secure" and "reliable" herein mean "reasonably tamper-proof" or "tamper-detectable", i.e., that it is assured that the authentic information elements are provided and associated in a reliable manner, for example by a non-interested third party or by a device or by a combination of both, and furthermore, that the associated authentication information is secured against fraudulent actions such as disassociation, modification, replacement etc., attempted by an interested party such as the sending or receiving party, at least to the extent that such actions are detectable.

The dispatch information can be any information describing at least the time and destination of the dispatch and preferably the dispatch completion status. Other information relating to the dispatch, such as the identity of the sender and/or the recipient, handshake information, the actual elapsed dispatch time, the number of pages dispatched and so forth. The identification of the authenticator, for example its name, logo, stamp, etc., can also be provided.

Finally, the authentication information can be secured or stored in a secure location or device, in its entirety or in part, together or separately, as desired.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description taken in conjunction with the drawings in which:

Fig. 1 is a schematic pictorial illustration of the authentication method of the present invention implemented in a manual manner;

Fig. 2 is a schematic illustration of an authenticator, constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 3 is a schematic illustration of an alternative authenticator, constructed and operative in accordance with another preferred embodiment of the present invention;

Fig. 4 is a schematic illustration of an alternative authenticator, constructed and operative in accordance with additional preferred embodiment of the present invention

Figs. 5 and 6 are schematic illustrations of verification mechanisms constructed and operative in accordance with the authenticator of Fig. 4;

Fig. 7 is a schematic illustration of an alternative authenticator, constructed and operative in accordance with yet another preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1 which illustrates the method of the present invention as it can be implemented for paper documents being sent non-electronically. The method of Fig. 1 can be implemented for documents sent via any document dispatching service, such as a courier service or the registered mail service of the post office.

The sender 10 provides the documents 12 to be sent and a destination address 14 to a clerk 20 of the document dispatching service. The clerk 20 prepares a dispatch sheet 26, which typically has a unique dispatch identifier (not shown) and has room for dispatch information such as the date and time of dispatch or delivery 16, the destination address 14, an indication 18 of proof of delivery such as the recipient's identity and/or signature, and optionally, additional dispatch information such as the dispatcher's signature and the identity of the sender 10, etc.

The clerk 20 fills in the dispatch sheet 26 with the date/time 16 and the address 14, and then prepares a copy 24 of the documents 12 and a copy 34 of the dispatch sheet 26, typically by utilizing a copy machine 22 or an electronic scanner. The clerk 20 then places the original documents 12 into an envelope 28 carrying the address 14, and sends the envelope 28 to its destination 30. In one embodiment of the present invention the dispatching service utilizes a cash-register like device to fill in the dispatch sheet 26. This provides for reliable time stamping and automated dispatch record keeping. Furthermore, the electronic dispatch information produced by such device can be associated using a special mathematical method as discussed in greater detail hereinbelow.

The clerk 20 associates the copy 24 of the documents 12 with the copy 34 of the dispatch sheet 26 by any method, a few examples of which follow:

a) by inserting the documents copy 24 and the dispatch sheet copy 34 into an envelope 32;

b) by inserting the copy 24 of the documents into an envelope 32 and marking the dispatch identifier on the outside of the envelope 32;

c) by printing the dispatch identifier on the documents copy 24; or

d) attaching the copies 24 and 34 and applying the stamp of the dispatch service in such a manner that part of the stamp is on the copy 24 of the documents and part of the stamp is on the copy 34 of the dispatch sheet 26.

Preferably, the clerk 20 secures the copies 24 and 34 in a manner that makes it difficult to modify or replace the information contained therein, for example by marking the pages of the copy 24 with the dispatching service's signature, stamp or seal, by spreading each page with invisible or other ink, by sealing the envelope 32 or by retaining them in the service's secure file 36 and so forth.

In one embodiment of the present invention, the associated copies 24 and 34 are provided to the sender at this stage (where the dispatch sheet 26 is retained with the service to ascertain delivery and to fill in the proof of delivery indication 18) or after the delivery is completed. In another embodiment, the dispatch service retains, in a secure location 36, one or both of the copies 24 and 34.

The clerk 20 can also identify the authenticating party, for example via his signature, or by having the dispatch sheet copy 34 printed on the stationary of the dispatching service, by stamping the documents and/or dispatch sheet copies with the service's stamp, logo or seal, etc.

When it is desired to authenticate the dispatch of the original documents (and possibly also their receipt at the destination 30), either the sender or the document dispatching service provides the associated authentication information, for example the envelope 32, unopened, to the party which required the authentication. When the envelope 32 is opened, it has associated therewith copies of both the dispatched documents and the dispatch information. The envelope 32 therefore, provides a reliable proof that the original documents 12 were dispatched on the date and to the destination listed on or in envelope 32.

It will be appreciated that, since a non-interested third party who is neither the sender nor the receiver copied the original documents 12 being sent, it is unlikely that the copies stored in the envelope 32 are other than copies of the original documents 12.

Various modifications can be made to the embodiment provided hereinabove without departing from the scope and spirit of the present invention. For example, the document copy could be sent to the destination while the original could be authenticated. The authentication information could be provided by the service, directly to the court of law. The document copy could be produced by a scanner or a camera and stored in an electronic or other storage device such as a disk or on microfilm, while a copy thereof is provided to the sender. The original dispatch sheet could be first filled out and then provided to the sender instead of using a copy. Moreover, the original documents could be scanned by the sender in the service's premises into a secure disk and one printed copy thereof could be sent by the service to the destination while another copy could be authenticated and provided to the sender. Alternatively, the documents could be provided to the service via transmission (e.g., by facsimile machine) rather than manually. In the case of a courier, the courier could produce the copy himself using a photocopier at the sender's premises, and so forth.

Reference is now made to Fig. 2 which illustrates an authenticator 70, constructed and operative in accordance with a preferred embodiment of the present invention, which can be part of a system for transmitting information, whether by facsimile machine, modem, computer, network or E-Mail stations, and any combinations thereof, or by other electronic means.

Fig. 2 illustrates a data communication system comprising a sending transceiver 42, a communication line 45, coupled to the sending transceiver 42, a communication network 44 and a receiving transceiver 46. Authenticator 70 of the present invention communicates at least with the sending transceiver 42, and can form part of the sending transceiver 42 or can be separated therefrom.

The sender provides original materials 40 for transmission, which can be paper documents or electronic information such as computer disk, memory and other electronic information including audio/video, text and graphics files or pictures. The sender also provides the destination address 52 which represents the address of the receiving transceiver 46 on communication network 44. The address 52 may for example be a dial number, a network user code and so forth. The sending transceiver 42 needs to transmit the information contents of the materials 40 to the receiving transceiver 46. To provide authentication, the transmission in Fig. 2 is performed through the authenticator 70 in a "store & forward" manner.

The authenticator 70 comprises input means 72 for receiving the transmitted information 60 and the destination address 62 from the communication line 45. The input means 72 may for example comprise a line interface, a Dual-Tone Multi Frequency (DTMF) decoder for receiving a destination address 62 such as a dial number, and a transceiver similar to that of the sending transceiver 42 which can receive the information 60.

The authenticator 70 also comprises an optional storage unit 54 such as a tape, disk or memory device and so forth for storing the information 60 and related dispatch information, an internal clock 50 for generating a time indication 66 of the transmission, a transceiver 76 for transmitting the information 60 to address 62 (the transceiver 76 can be used by the input unit 72 as well, for example by using a relay mechanism), a controller 56, a user interface 48, and an output unit 58 for providing the authentication information, for example to the sender.

The information 60 is then transmitted over the communication network 44 to the receiving transceiver 46 by the transceiver 76 using the address 62.

The internal clock 50 provides an indication 66 of the current time, and is utilized to provide a time indication for the transmission. Internal clock 50 is securable (to ensure the veracity of the produced time indication 66), and preferably provides time indications according to a non-changing time standard, such as Greenwich-Mean-Time (G.M.T.) or UTC. Alternatively, the time indication 66 can be externally obtained, for example from a communication network server, as long as the source is secured from being set or modified by an interested party such as the sender. The security of the time indication can be provided in a number of ways, such as by factory pre-setting the clock 50 and disabling or password securing the Set Date/Time function of the internal clock 50. Alternatively, the clock 50 can maintain a "true offset" with the true preset date/time, that reflects the offset of the user set date/time from the genuine preset one.

The transmission completion indication 64 provides information regarding the success of the transmission. It is typically obtained from the communication protocol used by the transceiver 76. It may be for example in the form of an electronic signal provided by the transceiver 76 which is used to determine the validity of the rest of authentication information, or in a form similar to that provided in transmission reports such as "TRANSMISSION OK" or "ERROR". In one embodiment of the present invention, the fact that the rest of authentication information elements are provided, indicates that an affirmative completion indication has been provided.

The storage unit 54 is used for storing the information 60 and/or the dispatch information, including the address 62, the time indication 66, and optionally the transmission completion indication 64. Typically, the storage unit 54 is relatively secure, such that the authentication information contained therein is assumed unchangeable. For example it may be a Write-Once-Read-Many (WORM) device such as an optical disk or a Programmable Read-Only Memory (PROM) device, it may be enclosed within a securable device, or it may be provided with read-only access privilege. Alternatively, the authentication information is stored in a secure manner, for example using a compression, private or public key encryption or scrambling technique, a password, or a combination thereof, such as those employed by the widely used RSA encryption method, and by the PKZIP(tm) program from PKWARE Inc., Glendale Wisconsin, U.S.A., and where the "securing" procedure, key or password are unknown to any interested party.

The controller 56 associates the information 60 and the dispatch information, by storing them in storage unit 54 and by associating link information with the stored authentication information, for example in the form of a unique dispatch identifier such as a sequential dispatch number.

To provide the authentication information for the transmission, the dispatch identifier is provided to the controller 56 through the user interface 48. The controller 56, in turn, retrieves the various stored authentication information elements from storage unit 54. If the stored information is also secured (i.e., by compression, password, etc.), the controller 56 "unsecures" them, and then provides them to the output unit 58.

The output unit 58 provides the authentication information to an output device (not shown). The authenticator 70 may include an output device or may communicate with some external unit. The output device can be, for example, a printing unit, a display unit, a storage unit such as a computer disk, the printing apparatus of the sending transceiver 42 and so forth.

The information 60 and the dispatch information, can be associated with each other in any suitable manner. For example, if the materials 40 provided for transmission are paper documents, one embodiment of the authenticator 70 authenticates the original documents by printing the dispatch information on them. In another embodiment, they can be stored in storage unit 54 together (e.g., sequentially or combined into a single file), or separately using a link information element (e.g., using a dispatch identifier). If the output is a printout, output unit 58 typically formats the printout to indicate the dispatch information on at least one, and preferably on all, of the pages containing the printout. Alternatively, a link information element, such as a dispatch identifier, can be printed on each printed page of the information 60, and separately on a dispatch page containing the dispatch information. Another method includes printing both the information 60 and the dispatch information together on contiguous paper, optionally between starting and ending messages, and so forth. An alternative special mathematical association method is discussed hereinbelow.

Typically, the authenticator 70 is relatively secure, such that the various devices and the authentication information elements enclosed therein can be assumed to be unchangeable. For example, the authenticator 70 can be enclosed within a password protected sealed electronic box which, if opened without authorization, may disable the normal operation of the authenticator 70, or may clearly indicate that it has been tampered with.

As mentioned hereinabove, the authenticator 70 can form part of the sending transceiver 42. Fig. 3 illustrates such an embodiment, which is similar to that of Fig. 2 and similar functional elements have similar reference numerals.

In Fig. 3, the input unit 72 of the sending transceiver 42 comprises means, for example a serial, parallel or disk interface, for inputting the information 60 and the destination address 62 from any component of the sending transceiver 42, for example from its input devices. The sending transceiver 42 replaces the transceiver 76 of Fig. 2. The storage unit 54 however is optional, as the information 60 and the related dispatch information could be provided to the output unit 58 "on-the-fly" in a manner similar to that used by the "copy" function of document facsimile machines.

Generally, in various embodiments of the authenticator 70, the information 60 can be obtained from any source and by any means, including a computer, a disk drive, a scanner or any other component of the sending transceiver 42, a communication line, a communication network and any combinations thereof, and so forth.

Furthermore, any information element having information content the substance of which is equivalent to that of the transmitted information can serve for authentication purposes, regardless of its form, representation, format or resolution, whether it is a paper document or electronic information, whether digital or analog, whether in form of dots and lines or alphanumeric, binary, hexadecimal and other characters, or whether it is encrypted, compressed or represented otherwise, and so forth. The element may contain additional information which does not change the substance and its content, such as a logo, a header message, etc. Furthermore, it may contain control, handshake and even noise data. Alternatively, an information descriptor such as a form number or name can be provided, and/or any other information content such as the form's filled-in data, which identifies the dispatched information.

Optionally, additional dispatch information may be provided to, or generated by authenticator 70, such as the number of pages transmitted, page numbers, the sender's identification, the sending transceiver's 42 identification, the receiving transceiver's 46 identification, the transmission elapsed time, a transmission identifier, integrity information such as a cyclic redundancy code (CRC), a checksum or the length of the transmitted information, an authenticator identification indication such as a serial number, a verification from the communication network 44 that the transmission has actually taken place at the specified time from the sender to the recipient's address, a heading message, a trailing message and so forth.

Typically, when the authenticator 70 comprises a reasonably secure storage unit 54, the stored information is retained therein and copies thereof are provided to the output unit 58. Preferably, the provided output or any part thereof is reasonably secured, so as to prevent any fraudulent action. For example, if the output is a printout, it can be secured by spreading invisible or other ink on it, or by using special ink, special print fonts or special paper to print the authentication information, or in any other suitable manner. Another method includes securing the dispatch information using, for example, an encryption technique, and printing the encrypted information on the printout. At a later stage the encrypted information can be decrypted to provide the true dispatch information, and so forth. Likewise, mathematical association method as discussed hereinbelow can also be used.

It will be appreciated that the following embodiments fall within the scope of the present invention:

The authenticator of the present invention can operate for information, such as a document produced by a word processor, transmitted through a computer. In this embodiment, the computer may include the secure time generator (which may for example be externally plugged into the parallel port). The authenticator obtains the dispatch information from the transceiver, and the document is provided from the hard disk or word processing program. The authenticator encrypts the document and the dispatch information together and stores them in a file. When authentication is required, the authenticator retrieves the stored file, decrypts it and provides the document and the dispatch information associated therewith to a printer.

Similarly, information transmitted in a computer network or electronic mail system can be authenticated, for example, by having a file server or mail manager (whose time generator is considered secure) store the transmitted information together with its associated dispatch information in a secure manner. One embodiment of secure storage is that which has read-only privileges. Alternatively, such read-only effect can also be obtained by having the authentication information encrypted with the authenticator's private key: everybody can decrypt it using the authenticator'a public key, but no interested party can change it without such action being detectable.

The present invention can be operated in conjunction with a message transmission forwarding service such as that provided by Graphnet Inc. of Teaneck, New Jersey, USA. The service obtains the information and address from the sender, typically by an electronic transmission, occasionally converts it (for example from ASCII text or word processor format into a transmissible document format) and forwards it to the requested address. The forwarding service serves as the authenticator and may for example provide the dispatch information associated with the transmitted information to the sender in a secure manner, such as in a sealed envelope or in encrypted form.

An efficient method for associating a plurality of information elements is by associating a digital representation thereof using a method referred to herein as "mathematical association". A digital representation of an information element can be considered as a number, for example as the element's standard binary, hexadecimal or other base representation. Using mathematical association, rather than maintaining the information elements (numbers) themselves, it is sufficient to maintain the results (also numbers) of one or more functions which are applied to one or more of these information elements. (These results are sometimes referred to as "message-digests", "hash-values" or "digital-signatures"). More formally, if A is a set of information elements, and F is the mathematical association function, then the set B of information elements is obtained as the result of applying the function F to the set A of information elements, i.e. B=F(A).

Preferably, the function F is selected such that a fraudulent attempt to change the elements of the set A, or an attempt to claim that a set A' which comprises different elements is the original set, can be readily detected by comparing the result B' obtained by applying the function F to the set A', to the original result B, i.e., by checking if F(A')=F(A).

It would be advantageous to select the function according to a cryptographic schemes. Encryption and digital envelope functions can provide for secure data interchange. Digital signatures can provide for accurate and reliable verification of both the signature generator and the data. One-way hash functions provides for security, and can reduce the size of the generated signatures while still enable verification of the original data used to generate these signatures. Utilizing combinations of cryptographic schemes can optimize particular implementations.

Various function classes of various degrees of complexity can be used for mathematical association purposes in accordance with various embodiments of the present invention. Furthermore, the function F and/or the result B can be kept secret and unknown in general, and to interested parties such as the sender or the recipient in particular. However, even if the function F and/or the result B are known, the task of finding a meaningful different set A' such that B=F(A') is mostly very difficult even for relatively simple functions, not to mention for more complex ones.

A special class of functions most suitable for the purposes of the present invention is the class of functions having the property that given the result B = F(A), it is exceptionally difficult to find a second set A' such that applying the function F to the second set A' will yield the same result B. The term "exceptionally difficult" refers herein to the fact that although many different such sets A' may exist, it is so difficult to find even one of them (sometimes even to find the set A itself) that it is practically infeasible. In fact, the functions of this class "hide" the elements they are applied to, (and sometimes the elements even cannot be reconstructed) and therefore this class is referred to herein as "the Hiding Class".

There are many advantages to using mathematical association in general, and functions of the Hiding Class in particular:

(a) It is efficient, for example for saving storage space and transmission bandwidth, to maintain a function result, the size of which is normally very small as compared to the original information elements themselves which can be arbitrarily large.

(b) It provides security, since the result is cryptic and there is no need to secure the information elements themselves. Furthermore, it is difficult, and sometimes infeasible to reconstruct the original elements.

(c) It provides a clear indication as to the authenticity of the elements of the set A used by the function to generate the result B. At any later time, the result B' obtained by applying the function F to a purported set A' can be compared to the original result B, and a match indicates beyond any reasonable doubt that set A' is same as the original set A. Moreover, integrity information such as the length of the information elements of the set A can be added and used as part of the set A, or the results of a plurality of functions can be maintained such that to make the task of finding such a different set A' infeasible.

(d) The result B' provided for comparison must be equal to the original result B, since any change to A will yield a different result B' with very high probability, and even if by chance a different set A' is found for which F(A')=B, the chance that it will be meaningful or will have the same length is practically zero.

(e) The function can be selected such that it is relatively easy and fast to compute the function result.

Few well known and widely used functions of the Hiding class are encryption functions (e.g., the RSA [1.06] or the DES [1.01] algorithms) and Cyclic-Redundancy-Check [3] (C.R.C.) functions (e.g., the C.R.C-32 function). While C.R.C functions are generally used in applications requiring verification as to the integrity of an arbitrarily long block of data, encryption is used to maintain the original data elements, though in different, cryptic representation. Encryption functions convert the information elements into one or more cryptic data blocks using one key, while enabling their reconstruction by providing a matching (same or different) key. Other well known members of this class of functions in the prior art are compression functions (e.g., the Lempel-Ziv 1977 [5] and 1978 algorithms), one-way hash functions [1.03] (e.g., the MD4 [4], and MD5 [1.04] algorithms), and MACs [1.13].

Since for authentication purposes there is no need to maintain the original information elements, the use of encryption functions (which normally maintain the information - though in a cryptic representation) may be inefficient. One-way hash functions (and other functions of the Hiding Class), on the other hand, maintain a small sized result value, but the information elements from which the result has been produced are secured, i.e., cannot be reconstructed therefrom. It would be more advantageous, for example, to apply a one-way hash function to the union of all the information elements, i.e., to a bit-string, where the leftmost bit is the leftmost bit of the first element, and the rightmost bit is the rightmost bit of the last element. This produces a cryptic and secure result, as described hereinabove. Furthermore, one-way hash functions can be computed relatively quickly and easily.

Generally and more formally, the result B is a set of one or more information elements b1,...,bm, where each element bi (which itself can comprise one or more information elements) is the result of applying a (possibly different) function Fi to a subset Si of a set A which comprises one or more information elements a1,...,an, where the various subsets Si are not necessarily disjoint or different, each subset Si includes at least a portion of one or more (or even all) of the electronic information elements of the set A, and where each function Fi can comprise one or more functions (i.e., Fi can be the composition of functions). Preferably, the functions Fi are members of the Hiding Class. The elements of such a subset Si are considered to be mathematically associated.

Assuming that the set A comprises five information elements a1,a2,a3,a4,a5, a few examples of mathematical association function Fi and their result set B follow: (the UNION function is denoted as U(x1,...,xk), which is an information element comprising a bit-string, where the leftmost bit is the leftmost bit of the element x1, and the rightmost bit is the rightmost bit of the element xk.)

(a) single element result set B

b1=F1(S1)=F1(a1,a4,a5) = a1/(a4+a5+1)

b1=F1(S1)=F1(a1,a3,a4) = ENCRYPT(U(a1,a3,a4))

b1=F1(S1)=F1(a1,a2,a3,a4,a5) = MD5(U(a1,a2,a3,a4,a5)) * C.R.C(a3) mod 5933333

b1=F1(S1)=F1(a1,a2,a3,a4,a5) = C.R.C(ENCRYPT(U(a1,a2)), COMPRESS(U(a2,a3,a4)), a1, a5)

b1=F1(S1)=F1(a1,a2,a3,a4,a5) = U(a1,a2,a3,a4,a5) mod p (where p is a large Prime number)

b1=F1(S1)=F1(a1,a2,a3,a4,a5) = ENCRYPT(MD5(U(a1,a2,a3,a4,a5)))

(b) multi-element result set B

B = [C.R.C(U(a1,a3)), a2/(a1+1), ENCRYPT(a5)]

b1=F1(S1)=F1(a1,a3) = C.R.C(a1,a3)

b2=F2(S2)=F2(a1,a2) = a2/(a1+1)

b3=F3(S3)=F3(a5) = ENCRYPT(a5)

The elements of two or more (not necessarily disjoint) subsets of set A can be associated with each other by associating the elements of the result set B which correspond to these subsets, either mathematically, or by non-mathematical methods, as described hereinabove. Furthermore, if there is a subset of elements of set A to which no function has been applied, these elements may be associated with the elements of the result set B, again either mathematically or by non-mathematical methods.

Moreover, the elements of two or more subsets of the set A can be associated with each other by associating the elements of each of these subsets with a common subset comprising one or more elements of the set A, where this common subset uniquely relates to the specific dispatch. This type of association is referred to herein as "indirect association", and the elements of this common subset are referred to herein as "link elements". A link element can be for example a unique dispatch number, or the subset comprising the time indication and a machine serial number, etc.

For example, assuming that the element a2 of the above set A uniquely relates to the dispatch, the following function generates a multi-element result set B:

$$B = [b1,b2,b3] = [ENCRYPT(a1,a2), COMPRESS(a2,a3,a4), a2+a5]$$

where the subsets Si include the following elements: S1=[a1,a2], S2=[a2,a3,a4] and S3=[a2,a5]. The elements of each subset are mathematically associated. Since all of these subsets include the common link-element a2, all their elements (in this case all the elements of the set A) are associated with each other.

Reference is now made to Fig. 4 which is a block diagram that illustrates an authenticator 100, constructed and operative in accordance with a preferred embodiment of the present invention. The authenticator 100 comprises a secure time generator 104, a storage device 106 and a function executor 102 which has means for inputting the following information elements: the transmitted information, the destination address, a time indication generated by the secure time generator 104, and a dispatch completion indication. Optionally, additional information elements can be provided as well.

The function executor 102 can be for example a Microchip Technology Inc.'s PIC16C5x series EPROM-based microcontroller, and the input means can be for example an I/O port, a serial, parallel or disk interface. The function executor 102 is capable of executing a function F on at least one, and preferably on the union of all of the input elements, and of generating a result information element which is provided to a storage device 106, and optionally to an output device 108, such as a printing device.

Preferably, the function F is a member of the Hiding Class, and is kept unknown at least to any interested part, by the function executor 102. This can be achieved for example by enabling the code protection feature of the PIC16C5x series microcontroller. Alternatively, a MAC [1.13] such as a one-way hash function MAC can be used where secret codes, keys and data relating to the function can be for example stored in a shielded memory device which is automatically erased if the authenticator 100 is tampered with. Also, preferably the storage device 106 is a WORM device, such as a PROM. Preferably, a different function is used for each device employing the function F. This can be achieved for example by using different keys or codes with each function.

In accordance with one embodiment of the present invention, the authenticator further comprises a verification mechanism for verifying the authenticity of a set of information elements purported to be identical to the original set of information elements. It is however appreciated that the verification mechanism can be separated therefrom.

Reference is now made to Fig. 5 which is a block diagram that illustrates a verification mechanism 120, constructed and operative in accordance with a preferred embodiment of the present invention, where at least part of the information elements were mathematically associated by the authenticator 100 of Fig. 4.

The verification mechanism 120 includes a function executor 122 for generating a new result information element according to the same function employed by the function executor 102 of Fig. 4. The function executor 122 has means for inputting information elements corresponding to the original information elements input to the function executor 102 of Fig. 4., and which are purported to be identical to those original elements.

The verification mechanism 120 also comprises a comparator 124, which has input means for inputting the newly generated result information element and the original result information element which may be obtained from the storage device 106 of Fig. 4, or manually, for example through a keyboard. The comparator 124 then compares the two provided result information elements to determine if they are the same, and the comparison result can be output for example to a display or printing unit. A match indicates that the purported information elements are authentic.

Reference is now made to Fig. 6 which is a block diagram that illustrates a verification mechanism 140, constructed and operative in accordance with a preferred embodiment of the present invention, where the information elements were associated non-mathematically, and are for example stored in storage unit 54 by the authenticator 70 of Fig. 2.

The verification mechanism 140 comprises a comparator 144, which has input means for inputting at least one of the stored associated information elements from the storage unit 54 of Fig. 2. The comparator 124 also has input means for inputting the corresponding information elements purported to be identical to the stored elements. The comparator 124 then compares the corresponding information elements to determine if they are the same, and the comparison result can be output for example to a display or printing unit. A match of all the compared elements indicates that the purported information elements are authentic.

It is appreciated that various embodiments of the present invention can include a combination of the verification mechanisms described hereinabove.

Also, part of the securing methods which were described for Fig. 2 include for example encryption and compression - methods which formally relate to mathematical association functions such as ENCRYPT(a1,...,aj) and COMPRESS(a1,...,aj). Occasionally, there is a need for reconstructing some or all of the secured mathematically associated information elements, for example for providing them to an output unit or to the comparator of the verification mechanism. Since some compression and encryption functions (as some other functions) are reversible, they are typically used when reconstruction of the elements is needed. (A function G is considered reversible if there exists a function H such that H(G(x))=x, and the function H is called the inverse function of G).

As discussed hereinabove, a mathematical association function can generally comprise a single function, or the composition of two or more functions. For example, the function ENCRYPT(a1,...,aj) comprises a single function - ENCRYPT, which is reversible, and its inverse function is DECRYPT. Another function COMPRESS(ENCRYPT(a1),C.R.C(a2,...,aj)) is the composition of three functions - COMPRESS, ENCRYPT and C.R.C, where the first two are reversible and their inverse function are DECOMPRESS (which yields the set comprising ENCRYPT(a1) and C.R.C(a2,...,aj)), and DECRYPT (which yields the element a1) respectively. The C.R.C function however, is not reversible.

Formally, if a function Fi comprises one or more functions, some of which are reversible, a set C comprising one or more information elements c1,...,ck can be generated, where this set C is expressive as a function I applied to the result information element bi of the function Fi, where this function I comprises the inverse function of one or more of these reversible functions.

While the authentication methods described hereinabove refer mostly to symmetric digital signatures, a preferred authentication method may be obtained using public-key digital signatures. A major advantage of public-key digital signatures over symmetric digital signatures is that they enable any third party (such as a judge), to verify the authenticity of both the data and the signer (where by using symmetric digital signatures, only a designated authenticator such as a secure device or a trusted third party, which have knowledge of the function, secret keys/codes etc., can perform the verification). The data is guaranteed not to be tampered with, and furthermore, once the data is signed, the signer is actually "committed" to it and cannot later repudiate his commitment to the digitally signed data, for only the signer which has sole knowledge of his private key could have created the signature, thus allowing such data to be legally binding.

Typically, public-key digital signatures generation and data authentication in performed in the following manner: a computation involving the signer's private key and the data, which can comprise various elements such as the dispatched message, the time indication, the destination address, and so forth is performed; the output is the digital signature, and may be attached to the data or separated therefrom. In later attempt of verification of the data, some computation involving the purported data, the signature, and signer's public key is performed. If the results properly hold in simple mathematical relation, the data is verified as genuine; otherwise, it may be forged or may have been altered or otherwise tampered with.

Since the signing process using the whole (plain) data is generally time consuming and the signature consumes a considerable amount of storage space, typically a relatively unique representation (also called a "fingerprint" or the "message digest") of the data is first generated using a process in which the data is "condensed" or "hashed", for example by means of a one-way hash function into a relative small value, thereby fixing its contents, and the signing process is performed on the fingerprint, resulting in an equivalent effective authentication. Therefore, the term digital signature herein refers to the digital signature of either the plain data element(s) or of any representation (function) thereof.

As described hereinabove, the fingerprint of a series of data elements can be generated thereby fixing their contents and associating them with each other. Since public-key digital signatures belong to the "Hiding Class", and since they further own the property that they can be generated with one key (such as the private key), and provide for later non-repudiable verification using another matching key (such as the public key), the usage of such functions for the purposes of the present invention is therefore of great advantage.

Reference is now made to Fig. 7 which is a block diagram that illustrates an E-Mail system 700, and a message dispatch and authentication service 750, constructed and operative in accordance with a preferred embodiment of the present invention. The sender 701 provides the E-Mail message 702 and the recipient's 799 E-Mail address 704 to the message dispatch and authentication service 750. Without limiting the generality, although reference is made to E-Mail dispatching services and systems in general, it is appreciated that implementations relating to the embodiments described herein can be easily extended, modified, ported or derived therefrom to other electronic data dispatch systems.

The dispatched message 702 may comprise any digital data such as text, pictorial, graphic, audio and video data, any number of files etc., in any signature 742 and optionally various dispatch information elements from which it has been generated (there is no need to provide the message 702 and address 704 since they are already with the sender 701), thus the certificate 740 is typically tiny.

Thus, for example, using RSA to generate the signature, if M is the dispatched message 702, A is the address 704, T is the time indication 720, I is the delivery information 708, and Ka is the authentication service's RSA private key, then the following is a sample calculation of S - the signature 742:

S = RSA(MD5(U(T,I,M,A)), Ka)

The certificate 740, which comprises the service's digital signature for the dispatch transaction, constitutes an non-repudiable evidence witnessed by the service for the dispatch and its contents, since the dispatched message contents is securely associated with the dispatch information (by means of the service's generated signature and/or fingerprint), and since the signature, the message and the dispatch information can at any later time be authenticated and verified by any third party both for integrity and originality by means of the service's public key (and if the message has also been signed by the sender, it can further be verified in the same manner using the sender's public key).

Thus, for example if PBKa is the service's public key, then by providing the above signature S - the purported message M', time indication T', address A' and delivery information I', can be authenticated by verifying that the following relation holds:

form or representation e.g., compressed, encrypted, plaintext etc. Preferably, the message 702 includes the sender's 701 digital signature, which the sender can generate by means of his private key, in order to establish the sender's "commitment" to the message 702, and to provide for verification of the message and sender as the message originator, any third party using the sender's public key.

Digital signatures can be generated in system 700 for example by means of a verifiable public-key algorithm such as RSA or DSA. Fingerprints can be generated for example by means of a one-way hash function such as MD4 or MD5.

The service 750 forwards the message 701 to the recipient 799 using the address 704. The service 750, preferably after assuring that the message has been successfully delivered, adds (e.g., appends) a dispatch time indication 720 to the message 702 and the address 704, as well as information 708 indicating the success (or failure) of the message delivery. Obviously, additional dispatch information elements, such as a sequential dispatch number, the sender, recipient and the service identification information and so forth may be added as well.

The service 750 then associates the above data elements for example by generating their fingerprint, which is then signed using the service's private key 752, to produce the service's signature 742. Signing the fingerprint can reduce the resulting signature 742 computation time, transmission bandwidth and storage space. The service then provides back to the sender 701 a service's generated certificate 740 comprising the service's

$$RSA(S, PBKa) = MD5(U(T',I',M',A'))$$

To increase the credibility of the system, a record of the certificate 740 can be kept with the service, and furthermore, a copy of the certificate 740 can be provided for storage to one or more trustees, such as a designated authority, or law and/or public accounting firms. Alternatively, the certificate 740 may itself be signed by one or more trustees, using their private keys.

A related embodiment can utilize a Time Stamping Service (TSS) such as the Digital Notary System (DNS) provided by Surety Technologies Inc. [1.10], which has been proposed by Haber et al. in their U.S. patent documents [2]. The certificate 740 or any portion thereof (such as the signature 742) can be sent to the DNS to be time stamped. Alternatively, an embodiment of the present invention could internally implement the DNS scheme. The DNS generates a certificate authenticating the certificate 740. Utilizing such time stamping schemes is of great advantage, since the DNS generated certificates are virtually unforgeable, and there is no need to deposit copies of the certificates with trustees. Since in this case the DNS time stamps the certificate 740 anyway, the service 750 itself optionally need not add the time indication 720.

Thus, for example, if C is the certificate 740 (not including the time indication 720), which comprises A, I, N and S (as defined above), and T is the time indication added by the DNS, then DNSC - the DNS generated certificate may be calculated as follows:

$$DNSC = DNS (C, T)$$

As mentioned above, the message 702 is preferably digitally signed with the sender's 701 private key, to enable authentication of the sender's identity as the message originator using the sender's public key, to establish the sender's non-repudiable commitment to the message, and to verify the message integrity.

Nevertheless, any other method can be used for identification and/or authentication of the sender, though such methods can sometimes be more vulnerable or less effective. One embodiment for example could utilize an hardware component (preferably secured) with the sender's unique identification information "burned-into". In another embodiment the service 750 can utilize various log-in procedures to identify and authenticate the sender when he logs-in to obtain service. Sample authentication protocols and schemes are described in [1.09] and [1.11].

Likewise, the identity of the recipient's 799 of the message can be authenticated in similar manners. This is useful for example when both the sender and the recipient log-into the same dispatch service for E-Mail transactions. However, the message 702 is frequently delivered to another E-Mail server (acting as the recipient's agent, where the recipient later logs-in, identifies himself and downloads his messages) rather than to the recipient himself.

In such embodiments, it might be sufficient to obtain proof of delivery from the receiving server, for example in form of a server's digitally signed certificate, which may for example comprise the server's identification information, a dispatch identifier, the recipient's address and preferably the message and so forth (or a fingerprint thereof) - while assuming that the message will eventually reach the recipient. Alternatively, a later proof of the final delivery may be obtained from that receiving server. Such delivery details as described above may be included in the delivery information 708.

In order to avoid potential disputes, as for example in case of contractual E-Mail correspondence, it may be useful to back up such correspondence by an agreement where the parties agree that delivery indication provided by the recipient's agent is to be considered an acceptable proof of delivery to the recipient. Alternatively, it may be agreed that multiple (two, three or more times of) certified dispatches of the message to be considered an acceptable proof of delivery and so forth.

In one preferred embodiment, the recipient (or its agent) may provide a counter-signature (using his private key) for the message, the sender's digital signature of the message, or the service's certificate or for any portions thereof. This may provide an ultimate evidence for the message dispatch, its contents, its time and its delivery to its destination. Thus if Ks, Kr, Ka are the private keys of the sender, the recipient (or his agent) and the authentication service 750 respectively, M is the dispatched message 702, T is the time indication 720, N is a sequential dispatch number, IDs and IDr are the identification information of the sender and recipient respectively, and A is the recipient's address 704, then the following sample calculations of S - the signature 742 can be performed:

1. S = RSA(Ka,MD5(U(N,A,T,M,IDs,IDr)))

2. S = RSA(Ka,MD5(U(T,M,M',R)))

3. S = RSA(Ka,MD5(U(N,T,A,M,M',R")))

4. S = RSA(Ka,MD5(U(T,M',R)))

5. S = DNS(T,MD5(U(M',R)))

where

M'= RSA(Ks,MD5(M))

R = RSA(Kr,MD5(U(M,N)))

R'= RSA(Kr,M')

R"= RSA(Kr,N)

Such incorporation of identification information relating to the sender 701, the recipient 799 or both (either by means of their digital signature, or otherwise) in the certificate generated by the service 750, can provide for more complete authentication of the entire dispatch transaction, and can be used as evidence for the dispatch and its contents by both the sender and the recipient.

BIBLIOGRAPHY AND REFERENCES

[1] "Applied Cryptography (2nd Edition)", (Schneier Bruce, John Wiley & Sons, 1996).

[1.01] see [1] Chapter 12, pp. 265-301.

[1.02] see [1] Chapter 13 Section 13.9, pp. 319-325.

[1.03] see [1] Chapter 18 Section 18.1, pp. 429-431.

[1.04] see [1] Chapter 18 Section 18.5, pp. 436-441.,

see also "One-Way Hash Functions," (B. Schneier, Dr. Dobb's Journal M&T Publishing Inc., September 1991 Vol 16 No.9 pp. 148-151),

see also Internet Request For Comments (RFC) document 1321.

[1.05] see [1] Chapter 19 Section 19.1, pp. 461-462.

[1.06] see [1] Chapter 19 Section 19.3, pp. 466-474, see also "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (Rivest, R.L., A. Shamir, and L. Adelman, Communications of the ACM, ACM Inc., February 1978 Vol 21 No. 2, pp. 120-126).

[1.07] see [1] Chapter 20 Section 20.1, pp. 483-494,

see also "The Digital Signature Standard proposed by the National Institute of Standards and Technology" (Communications of the ACM, ACM Inc., July 1992 Vol 35 No. 7 pp. 36-40),

[1.08] see [1] Chapter 24 Section 24.12, pp. 584-587.

[1.09] see [1] Chapter 3 Section 3.2, pp. 52-56.

[1.10] see [1] Chapter 4 Section 4.1, pp. 75-79.

[1.11] see [1] Chapter 21, pp. 503-512.

[1.12] see [1] Chapter 2, Sections 2.6-2.7, pp. 34-44,

see also [1] Chapter 20, pp. 483-502.

[1.13] see [1] Chapter 18, Section 18.4, pp. 455-459.

[2] U.S. Patent Documents #5,136,646, #5,136,647, and #5,373,561.

[3] "Cyclic Redundancy Checksums (Tutorial)" (Louis, B. Gregory, C Users Journal, R & D Publications Inc., Oct 1992 v10 n10 p55 (6)), see also "File verification using C.R.C." (Nelson, Mark R., Dr. Dobb's Journal, M&T Publishing Inc., May 1992 Vol 17 No. 5 p64(6)).

[4] "The MD4 Message Digest Algorithm" (R. L. Rivest, Crypto '90 Abstracts, Aug. 1990, pp. 301-311, Springer-Verlag).

[5] "A Universal Algorithm for Sequential Data Compression" (Ziv. J., Lempel A., IEEE Transactions On Information Theory, Vol 23, No. 3, pp. 337-343).

The references and publications described by the above-mentioned articles are incorporated herein by reference.

While the present invention has been described with reference to a few specific embodiments, the description is illustrative of the invention and is not to be construed as limiting the invention. It is appreciated that various combinations, modifications and implementations relating to or derived from the embodiments described herein may occur to those skilled in the art without departing from the scope and spirit of the invention as defined by the appended claims.

WHAT IS CLAIMED IS:

1. Apparatus for authenticating that a sender has transmitted certain information via a dispatcher to an address of a recipient, the apparatus comprising:

means for providing a set A comprising a plurality of information elements a1,...,an, said information element a1 having information content the substance of which is equivalent to that of said transmitted information, and said one or more information elements a2,...,an having dispatch information, where at least one of said information elements is provided in a reliable manner; and

means for associating at least a subset of said dispatch information elements a2,...,an with said information element a1, such that said associated information is secured against fraudulent actions attempted at least by an interested party, in a manner that such actions are at least detectable.

2. Apparatus according to claim 1, wherein said means for associating comprises means for generating a new set B comprising one or more information elements b1,...,bm, each element bi of said new set B being expressive as a function Fi of a subset Si comprising at least a portion of a digital representation of at least one information element of said set A, and where said functions Fi can be different.

3. Apparatus according to claim 2, wherein said means for associating further comprises means for associating at least one information element of said new set B, with at least one information element of said set A.

4. Apparatus according to any of claims 2 or 3, wherein said set B comprises a plurality of elements, and wherein said means for associating further comprises means for associating at least two elements of said set B.

5. Apparatus according to claim 2, wherein said function Fi has the property that it is substantially difficult to find a set S' comprising at least one information element, said set S' being different from said subset Si of said set A and yet can be used instead, such that applying said function Fi to said set S' will yield said element bi, i.e., such that Fi(S')=bi.

6. Apparatus according to claim 2, wherein said function Fi comprises one or more functions.

7. Apparatus according to claim 2, wherein at least one member of the group comprising the following members: said function Fi, and at least one information element of said new set B, is un known at least to an interested party.

8. Apparatus according to any of claims 2 or 6, wherein said function Fi comprises at least one reversible function, and further comprising means for generating a set C comprising one or more information elements c1,...,ck expressive as a function I of at least said information element bi, where said function I comprises the inverse function of at least one of said reversible functions.

9. Apparatus according to any of claims 1, 2 or 8, and further comprising means for verifying the authenticity of a set V1 comprising one or more information elements which are purported to be identical to the corresponding elements of a subset V2 comprising information elements of said set A, said verification means comprising:

means for providing said purported information elements of said set V1;

means for providing said information elements of said subset V2; and

means for comparing said purported information elements of said set V1 with said corresponding information elements of said subset V2 to determine if they are the same.

10. Apparatus according to any of claims 2 or 8, and further comprising means for verifying the authenticity of a set V3 comprising one or more information elements which are purported to be identical to the

corresponding elements of said subset Si of said set A, said verification means comprising:

means for providing said purported information elements of said set V3;

means for generating a new information element bi' being expressive as said function Fi applied to said purported information elements of said set V3;

means for providing said element bi; and

means for comparing said elements bi' and bi to determine if they are the same.

11. Apparatus according to any of claims 9 or 10, wherein said means for verifying is separated therefrom.

12. Apparatus according to any of claims 1 or 2, and further comprising means for providing, at least to an interested party, at least one information element of the group comprising said associated information elements and the elements of said set B.

13. Apparatus according to any of claims 1 or 2, and further comprising means for storing at least one information element of the group comprising said associated information elements and the elements of said set B.

14. Apparatus according to any of claims 1 or 2, and further comprising means for securing at least one information element of the group comprising said associated information elements and the elements of said set B.

15. Apparatus according to claim 1, wherein said dispatch information includes at least one element of the group comprising the following elements: the date associated with said transmission, the time associated with said transmission, the address associated with said transmission, and a completion indication associated with said transmission.

16. Apparatus according to any of claims 1 or 15, wherein said dispatch information includes at least one element of the group comprising the following elements: the number of pages transmitted, page number, indication of said sender identification, indication of said recipient identification, said transmission duration, integrity information, indication of said transmission identification, indication of said authentication apparatus identification, a heading message, and a trailing message.

17. Apparatus according to claim 1, wherein said information elements have form selected from the group comprising the following forms: a paper document and electronic information.

18. Apparatus according to any of claims 1 or 17, wherein the source of said dispatched information provided for transmission has a form selected from a group comprising the following form: a paper document and electronic information.

19. Apparatus according to claim 18, wherein said information element a1 is said source.

20. Apparatus according to any of claims 1 or 2, wherein said dispatch information includes at least one link information element, wherein said means for associating comprises means for associating said link information element with at least one of said information elements, and for associating it with at least one another information element.

21. Apparatus according to any of claims 1, 15 , 16 or 20, and further comprising means for preparing at least one of said information elements.

22. Apparatus according to claim 21, further comprising a time indication generator which provides at least one of said time and said date associated with said transmission, where said time indication cannot be set or modified at least by an interested party.

23. Apparatus according to claim 1, wherein said dispatcher comprises at least one element of the following group: a facsimile machine, a modem, a

network interface card (NIC), a computer, a communication line, and a communication network.

24. Apparatus according claim 1, further comprising means for providing said transmitted information to said dispatcher.

25. Apparatus according to claim 1, wherein said apparatus is part of said dispatcher.

26. Apparatus according to claim 1, wherein said apparatus is relatively secure, such that any fraudulent action can at least be detected.

27. A method for authenticating that a sender has dispatched certain information via a dispatcher to an address of a recipient, the method comprising the steps of:

providing a set A comprising a plurality of information elements a1,...,an, said information element a1 having information content the substance of which is equivalent to that of said dispatched information, and said one or more information elements a2,...,an having dispatch information, where at least one of said information elements is provided in a reliable manner; and

having an authenticator associate at least a subset of said dispatch information elements a2,...,an with said information element a1, such that said associated information is secured against fraudulent actions attempted at least by an interested party, in a manner that such actions are at least detectable.

28. A method according to claim 27, wherein said dispatch information includes at least one element of the group comprising the following elements: the date associated with said dispatch, the time associated with said dispatch, the address associated with said dispatch, and a completion indication associated with said dispatch.

29. A method according to any of claims 27 or 28, wherein said dispatch information includes at least one element of the group comprising the following elements: the number of pages dispatched, page number, indication of said sender identification, indication of said recipient identification, said dispatch duration, integrity information, indication of said dispatch identification, indication of said authenticator identification, a heading message, and a trailing message.

30. A method according to claim 27, wherein the source of said dispatched information provided for dispatch has a form selected from a group comprising the following form: a paper document and electronic information.

31. A method according to claim 30, wherein said information element a1 is said source.

32. A method according to claim 27, wherein said dispatched information has a form selected from the group comprising the following forms: a paper document and electronic information.

33. A method according to claim 32, wherein said information is dispatched by a dispatching service which is selected from the following group: a courier service and the registered mail service of the post office.

34. A method according to claim 32, wherein said information is dispatched by transmission.

35. A method according to claim 34, wherein said dispatcher comprises at least one element of the following group: a facsimile machine, a modem, a network interface card (NIC), a computer, a communication line, a communication network, an E-Mail system, an EDI system, and a transmission service.

36. A method according to claim 27, further comprising the step of providing said dispatched information to said dispatcher.

37. A method according to claim 27, wherein said authenticator is selected from a group comprising an independent, non-interested third party, said dispatcher, a device, and any combination thereof.

38. A method according to claim 27, wherein said information element a1 comprises an information content of said dispatched information.

39. A method according to any of claims 27 or 32, further comprising the step of preparing at least one element of the group comprising the elements of said set A, and said dispatched information.

40. A method according to claim 39, wherein said dispatched information is prepared from a source selected from a group comprising the following elements: a paper document and electronic information.

41. A method according to claim 27, wherein said information elements have form selected from the group comprising the following forms: a paper document and electronic information.

42. A method according claim 27, further comprising the step of dispatching said information to said address of said recipient.

43. A method according to any of claims 27 or 39, wherein said step of associating comprises the step of generating a new set B comprising one or more information elements b1,...,bm, each element bi of said new set B being expressive as a function Fi of a subset Si comprising at least a portion of a digital representation of at least one information element of said set A, and where said functions Fi can be different.

44. A method according to claim 43, wherein said step of associating further comprises the step of associating at least one information element of said new set B, with at least one information element of said set A.

45. A method according to any of claims 43 or 44, wherein said set B comprises a plurality of elements, and wherein said step of associating further comprises the step of associating at least two elements of said set B.

46. A method according to claim 43, wherein said function Fi has the property that it is substantially difficult to find a set S' comprising at least one information element, said set S' being different from said subset Si of said set A yet can be used instead, such that applying said function Fi to said set S' will yield said element bi, i.e., such that Fi(S')=bi.

47. A method according to claim 43, wherein said function Fi comprises one or more functions.

48. A method according to claim 43, wherein at least one member of the group comprising the following members: said function Fi, and at least one information element of said new set B, is unknown at least to an interested party.

49. A method according to any of claims 43 or 47, wherein said function Fi comprises at least one reversible function, and further comprising

the step of generating a set C comprising one or more information elements c1,...,ck expressive as a function I of at least said information element bi, where said function I comprises the inverse function of at least one of said reversible functions.

50. A method according to any of claims 27, 43 or 49, further comprising the step of verifying the authenticity of a set V1 comprising one or more information elements which are purported to be identical to the corresponding elements of a subset V2 comprising information elements of said set A, said verification step comprising the steps of:

providing said purported information elements of said set V1;

providing said information elements of said subset V2; and

comparing said purported information elements of said set V1 with said corresponding information elements of said subset V2 to determine if they are the same.

51. A method according to any of claims 43 or 49, further comprising the step of verifying the authenticity of a set V3 comprising one or more information elements which are purported to be identical to the corresponding elements of said subset Si of said set A, said verification step comprising the steps of:

providing said purported information elements of said set V3;

element with at least one of said information elements, and the step of associating it with at least one another information element.

56. Apparatus according to claim 2, wherein said new set B comprises a verifiable digital signature of said subset Si of said set A.

57. Apparatus according to claim 56, further comprising a corresponding verification means for said verifiable digital signature, for authenticating at least one of the following: at least one element of said subset Si of said set A, and the originator of said digital signature.

58. Apparatus according to claim 56, wherein said digital signature is generated according to a scheme selected from the group comprising: secret-key (symmetric) cryptosystem, and public-key cryptosystem.

59. Apparatus according to any of claims 1 or 2, wherein said means for associating comprises means for time-stamping at least one information element of the group comprising said associated information elements and the elements of said set B, according to a Time Stamping Service scheme.

60. Apparatus according to any of claims 1, 2 or 16, further comprising means for authenticating the identity of at least one member of the group comprising: said sender, said recipient, an agent of said sender, and an agent of said recipient.

generating a new information element bi' being expressive as said function Fi applied to said purported information elements of said set V3;

providing said element bi; and

comparing said elements bi' and bi to determine if they are the same.

52. A method according to any of claims 27 or 43, further comprising the step of providing to an interested party at least one information element of the group comprising said associated information elements and the elements of said set B.

53. A method according to any of claims 27 or 43, further comprising the step of storing at least one information element of the group comprising said associated information elements and the elements of said set B.

54. A method according to any of claims 27 or 43, further comprising the step securing at least one information element of the group comprising said associated information elements and the elements of said set B.

55. A method according to any of claims 27 or 43, wherein said dispatch information includes at least one link information element, wherein said step of associating comprises the step of associating said link information

61. A method according to claim 43, wherein said new set B comprises a verifiable digital signature of said subset Si of said set A.

62. A method according to claim 61, further comprising a corresponding verification step for said verifiable digital signature, for authenticating at least one of the following: at least one element of said subset Si of said set A, and the originator of said digital signature.

63. A method according to claim 61, wherein said digital signature is generated according to a scheme selected from the group comprising: secret-key (symmetric) cryptosystem, and public-key cryptosystem.

64. A method according to any of claims 27 or 43, wherein said step of associating comprises the step of time-stamping at least one information element of the group comprising said associated information elements and the elements of said set B, according to a Time Stamping Service scheme.

65. A method according to any of claims 27, 29 or 43, further comprising the step of authenticating the identity of at least one member of the group comprising: said sender, said recipient, an agent of said sender, and an agent of said recipient.

Mark M. Friedman
Advocate, Patent Attorney
Beit Samueloff
7 Haomanim
67897 Tel Aviv

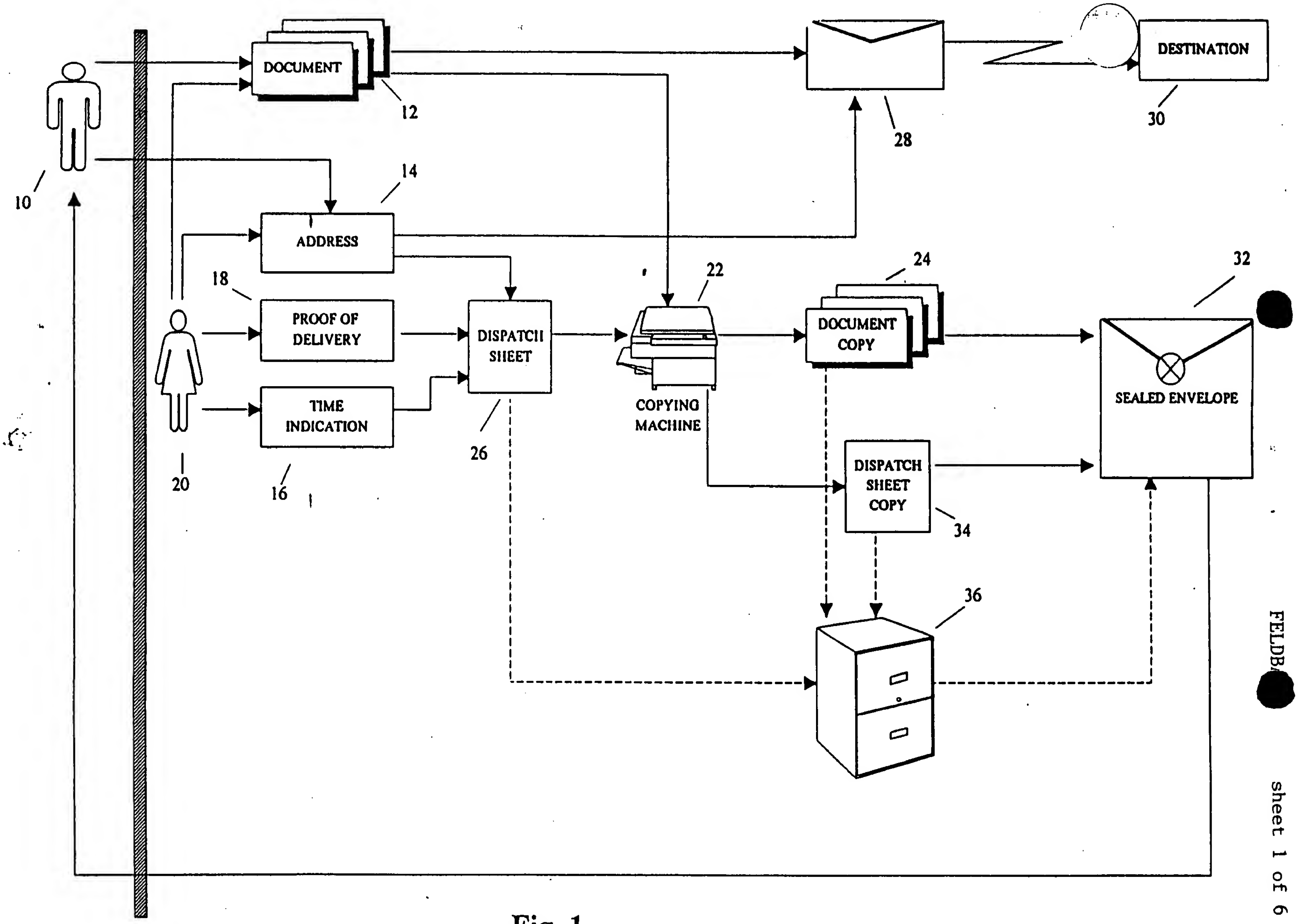

10
DOCUMENT
12
DESTINATION
30
28
14
ADDRESS
18
PROOF OF DELIVERY
TIME INDICATION
20
16
DISPATCH SHEET
26
22
COPYING MACHINE
24
DOCUMENT COPY
32
SEALED ENVELOPE
DISPATCH SHEET COPY
34
36

Fig. 1

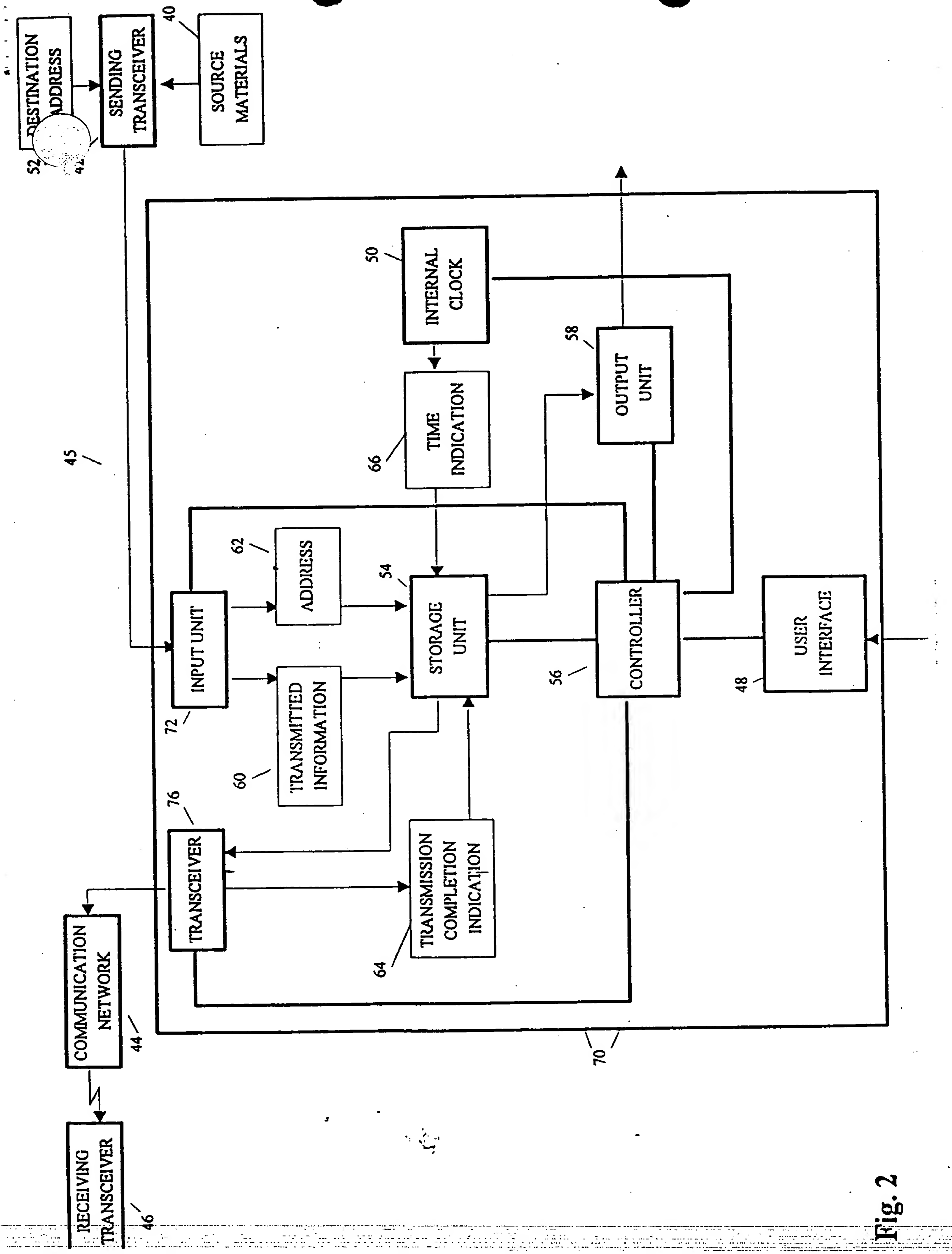

DESTINATION ADDRESS
52
42
SENDING TRANSCEIVER
40
SOURCE MATERIALS
45
INTERNAL CLOCK
50
TIME INDICATION
66
OUTPUT UNIT
58
ADDRESS
62
STORAGE UNIT
54
INPUT UNIT
72
TRANSMITTED INFORMATION
60
CONTROLLER
56
USER INTERFACE
48
TRANSCEIVER
76
TRANSMISSION COMPLETION INDICATION
64
COMMUNICATION NETWORK
44
70
RECEIVING TRANSCEIVER
46

Fig. 2

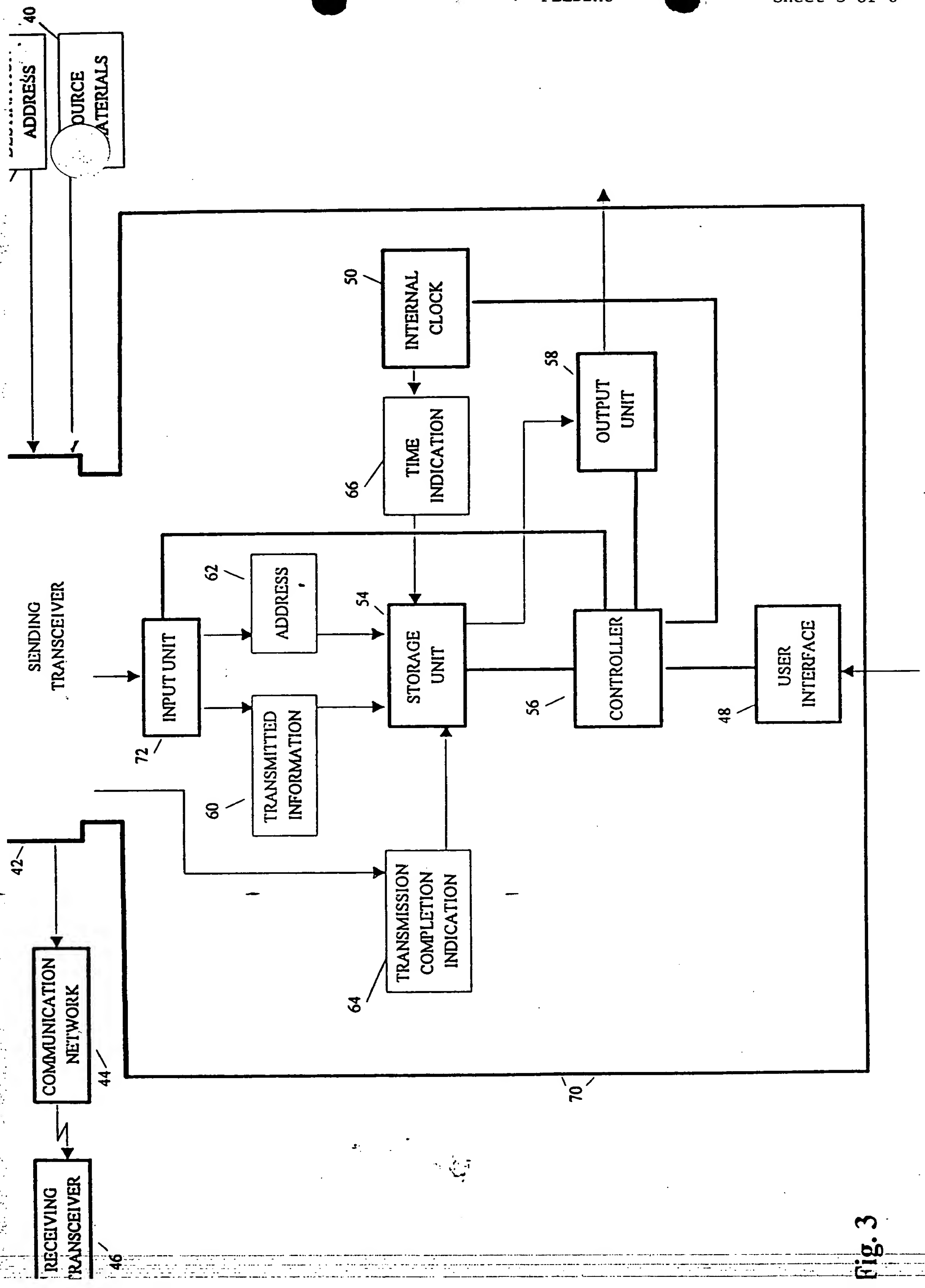

40
ADDRESS
OURCE
ATERIALS
SENDING TRANSCEIVER
INPUT UNIT
72
62
ADDRESS
60
TRANSMITTED INFORMATION
54
STORAGE UNIT
66
TIME INDICATION
50
INTERNAL CLOCK
64
TRANSMISSION COMPLETION INDICATION
58
OUTPUT UNIT
56
CONTROLLER
48
USER INTERFACE
42
44
COMMUNICATION NETWORK
46
RECEIVING TRANSCEIVER
70

Fig. 3

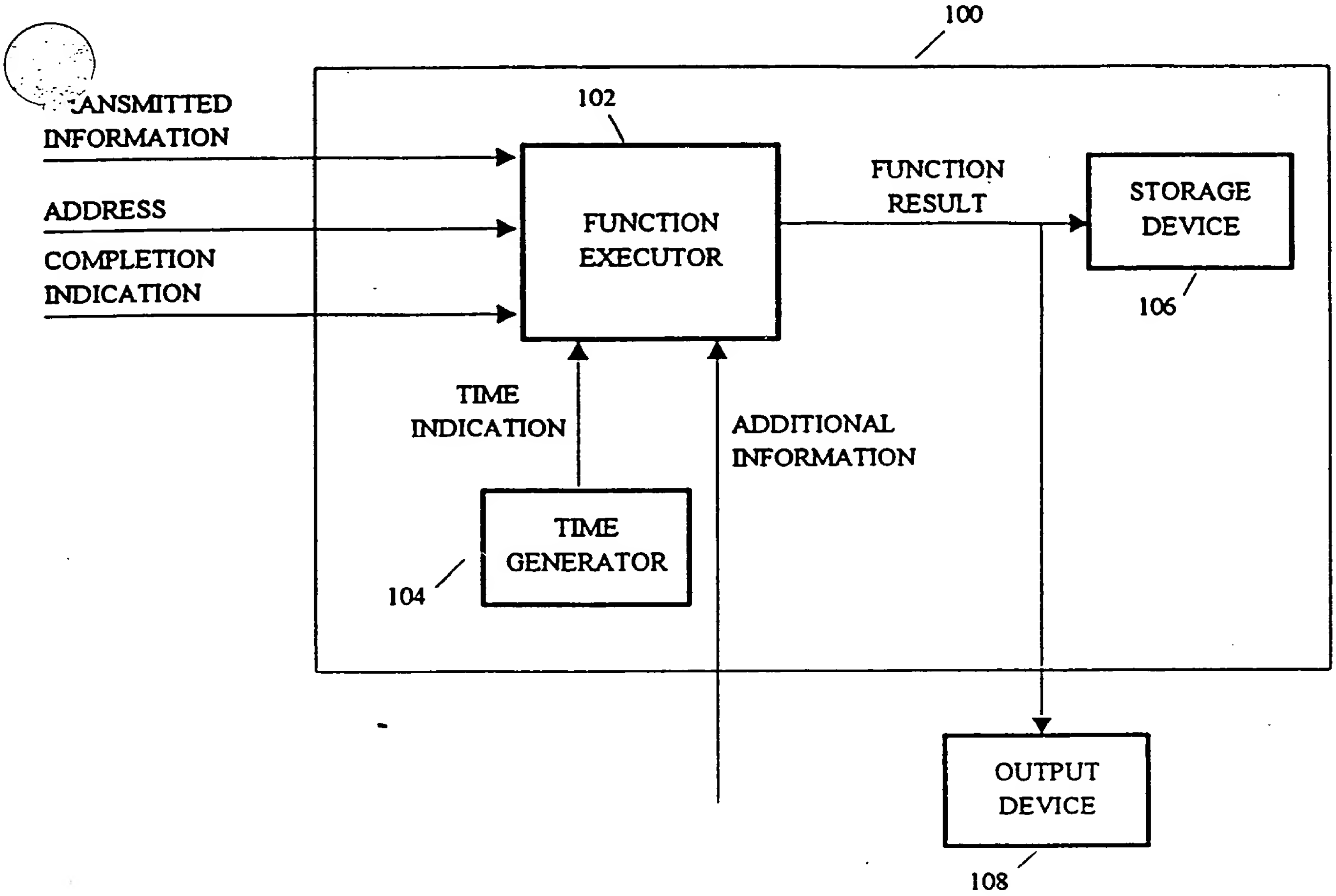

100
102
ANSMITTED INFORMATION
ADDRESS
COMPLETION INDICATION
FUNCTION EXECUTOR
FUNCTION RESULT
STORAGE DEVICE
106
TIME INDICATION
ADDITIONAL INFORMATION
TIME GENERATOR
104
OUTPUT DEVICE
108

FIG. 4

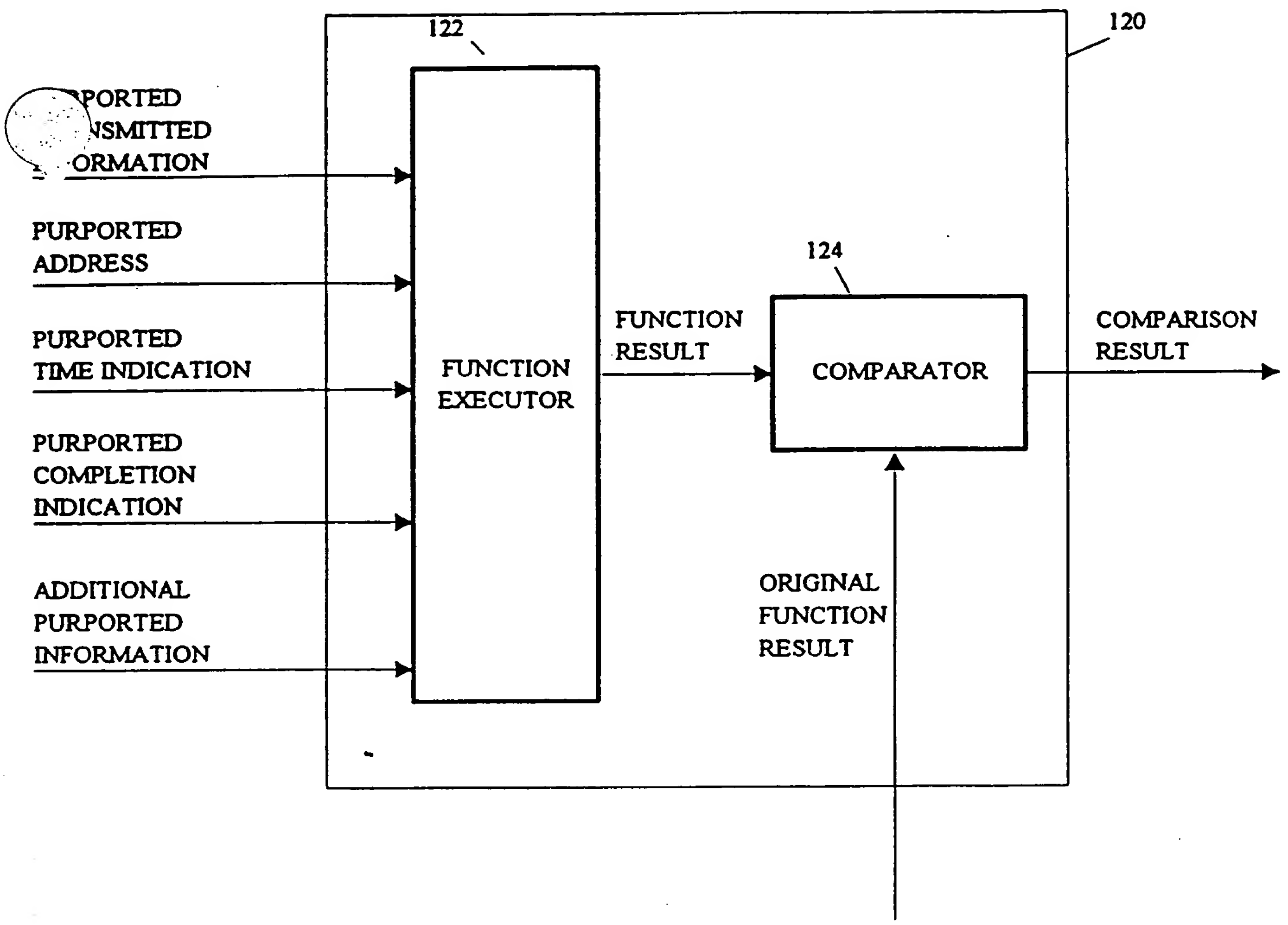

122
120
PURPORTED TRANSMITTED INFORMATION
PURPORTED ADDRESS
PURPORTED TIME INDICATION
PURPORTED COMPLETION INDICATION
ADDITIONAL PURPORTED INFORMATION
FUNCTION EXECUTOR
FUNCTION RESULT
124
COMPARATOR
COMPARISON RESULT
ORIGINAL FUNCTION RESULT

FIG. 5

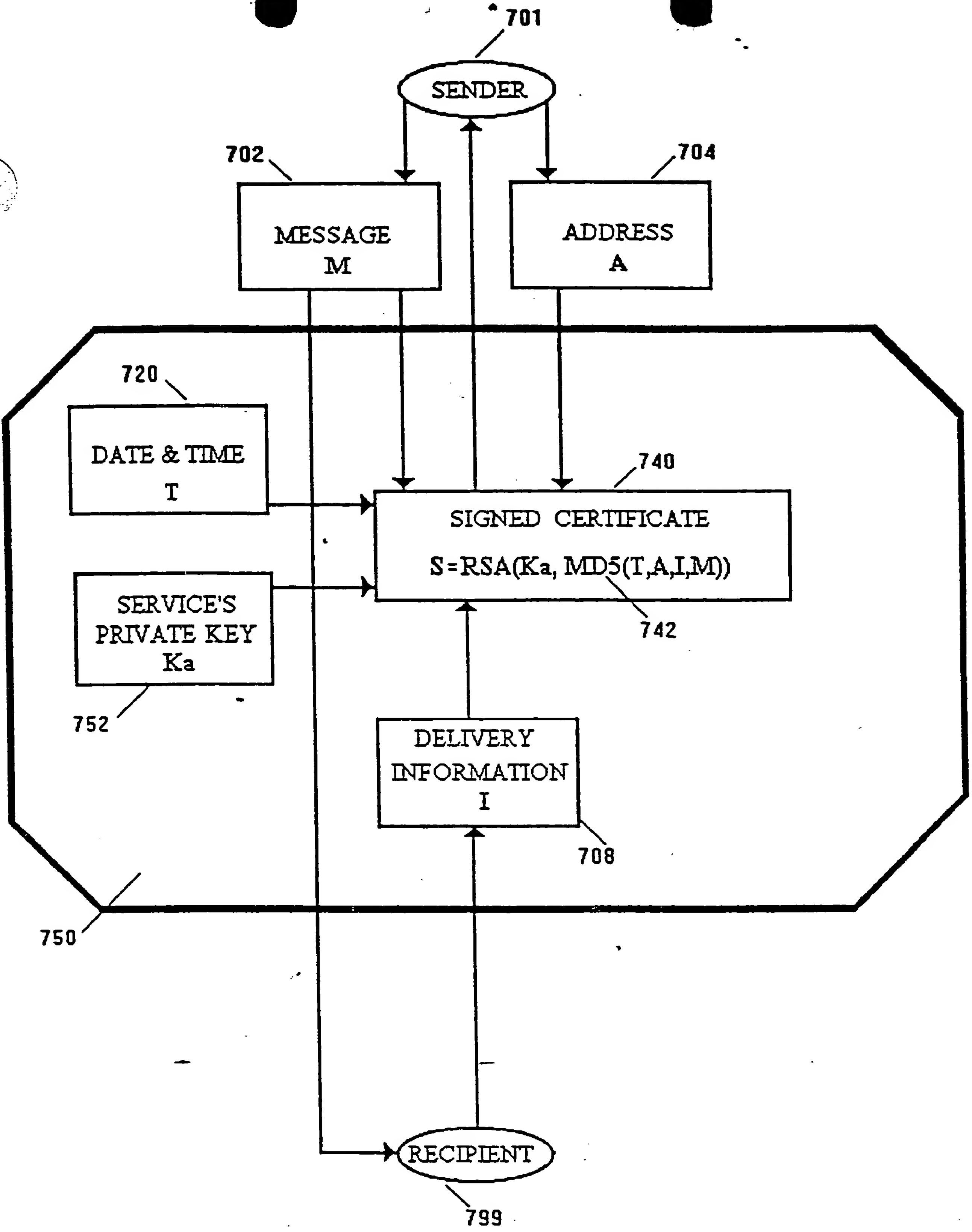


Fig. 7

E-MAIL AUTHENTICATION SERVICE
USING DIGITAL SIGNATURES

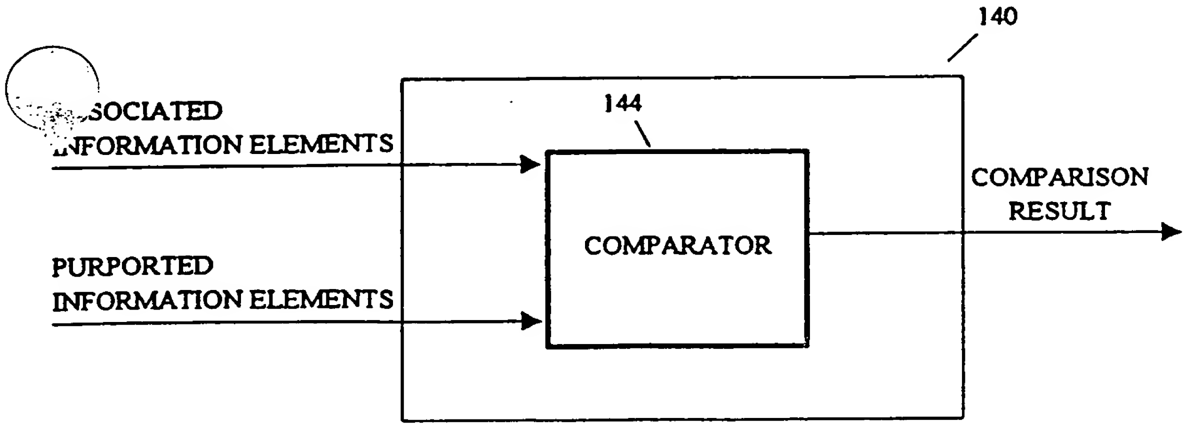

140
144
ASSOCIATED INFORMATION ELEMENTS
PURPORTED INFORMATION ELEMENTS
COMPARATOR
COMPARISON RESULT

FIG. 6